

Management Software

AT-S63



Web Browser Interface User's Guide

AT-9424T/SP AND AT-9424T/GB
LAYER 2+ GIGABIT ETHERNET SWITCHES

VERSION 1.0.0

PN 613-50592-00 Rev A



Copyright © 2004 Allied Telesyn, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Figures	9
Tables	13
Preface	15
How This Guide is Organized	15
Document Conventions	17
Where to Find Web-based Guides	18
Contacting Allied Telesyn	19
Online Support	19
Email and Telephone Support	19
For Sales or Corporate Information	19
Management Software Updates	20
Chapter 1	
Overview	21
Management Overview	22
Local Management Session	24
Telnet Management Session	25
Web Browser Management Session	26
SNMP Management Session	27
Management Access Levels	28
Section I	
Basic Features	29
Chapter 2	
Starting a Web Browser Management Session	31
Starting a Web Browser Management Session	32
Web Browser Tools	35
Saving Your Parameter Changes	36
Quitting a Web Browser Management Session	37
Chapter 3	
Basic Switch Parameters	39
Configuring an IP Address and Switch Name	40
Activating the BOOTP and DHCP Client Software	43
Displaying System Information	44
Configuring the Manager and Operator Passwords	46

Rebooting a Switch	48
Pinging a Remote System	49
Returning the AT-S63 Management Software to the Factory Default Values	50
Chapter 4	
SNMPv1 and SNMPv2c	53
Enabling or Disabling SNMP Management	54
Creating a New SNMPv1 and SNMPv2c Community	56
Modifying an SNMPv1 and SNMPv2c Community	59
Deleting an SNMPv1 and SNMPv2c Community	61
Displaying the SNMPv1 and SNMPv2c Communities	62
Chapter 5	
Enhanced Stacking	65
Setting a Switch's Enhanced Stacking Status	66
Selecting a Switch in an Enhanced Stack	68
Returning to the Master Switch	71
Displaying the Enhanced Stacking Status	72
Chapter 6	
Port Parameters	73
Configuring Port Parameters	74
Displaying Port Status	81
Displaying Port Statistics	85
Resetting a Port to the Default Settings	88
Chapter 7	
MAC Address Table	89
Adding Static Unicast and Multicast MAC Addresses	90
Deleting Unicast and Multicast MAC Addresses	92
Deleting All Dynamic MAC Addresses	93
Displaying the MAC Address Tables	94
Changing the Aging Time	97
Chapter 8	
Port Trunking	99
Creating a Port Trunk	100
Modifying a Port Trunk	103
Deleting a Port Trunk	105
Displaying the Port Trunks	106
Chapter 9	
Port Mirroring	109
Creating a Port Mirror	110
Modifying a Port Mirror	113
Disabling a Port Mirror	114
Deleting a Port Mirror	115
Displaying the Port Mirror	116
Section II	
Advanced Features	119
Chapter 10	
File Downloads and Uploads	121
Downloading a File	122
Uploading a File	125

Chapter 11	
Event Log	127
Enabling or Disabling the Event Log	128
Displaying Events	130
Disabling the Event Log	137
Clearing the Event Log	138
Saving the Event Log to a File	139
Chapter 12	
Quality of Service	141
Configuring CoS	142
Mapping CoS Priorities to Egress Queues	145
Configuring Egress Scheduling	148
Displaying the CoS Settings	150
Displaying the QoS Schedule	152
Chapter 13	
IGMP Snooping	153
Configuring IGMP Snooping	154
Displaying a List of Host Nodes	157
Displaying a List of Multicast Routers	160
Chapter 14	
STP and RSTP	163
Enabling or Disabling a Spanning Tree Protocol	164
Configuring STP	166
Displaying the STP Settings	170
Resetting STP to the Default Settings	172
Configuring RSTP	174
Resetting RSTP to the Default Settings	178
Displaying RSTP Settings	178
Chapter 15	
MSTP	181
Enabling MSTP	182
Configuring MSTP	184
Configuring MSTP Parameters	184
Configuring the CIST Priority	187
Creating, Deleting, or Modifying MSTI IDs	189
Creating an MSTI ID	189
Deleting an MSTI ID	190
Modifying an MSTI ID	190
Adding, Removing, or Modifying VLAN Associations to MSTIs	192
Adding a VLAN Association	192
Removing a VLAN Association	192
Modifying a VLAN Association	193
Configuring MSTP Port Parameters	195
Displaying the MSTP Port Configuration	197
Displaying the MSTP Port Status	200
Resetting MSTP to the Default Settings	202
Chapter 16	
SNMPv3	203
Configuring the SNMPv3 Protocol	204
Enabling or Disabling SNMP Management	205
Configuring the SNMPv3 User Table	207
Creating a User Table Entry	207
Deleting a User Table Entry	210

Modifying a User Table Entry	211
Configuring the SNMPv3 View Table	214
Creating a View Table Entry	214
Deleting a View Table Entry	217
Modifying a View Table Entry	218
Configuring the SNMPv3 Access Table	220
Creating an Access Table	220
Deleting an Access Table Entry	224
Modifying an Access Table Entry	224
Configuring the SNMPv3 SecurityToGroup Table	227
Creating a SecurityToGroup Table Entry	227
Deleting a SecurityToGroup Table Entry	230
Modifying a SecurityToGroup Table Entry	230
Configuring the SNMPv3 Notify Table	233
Creating a Notify Table Entry	233
Deleting a Notify Table Entry	235
Modifying a Notify Table Entry	236
Configuring the SNMPv3 Target Address Table	238
Creating a Target Address Table Entry	238
Deleting a Target Address Table Entry	241
Modifying Target Address Table Entry	242
Configuring the SNMPv3 Target Parameters Table	245
Creating a Target Parameters Table Entry	245
Deleting a Target Parameters Table Entry	248
Modifying a Target Parameters Table Entry	249
Configuring the SNMPv3 Community Table	252
Creating an SNMPv3 Community Table Entry	252
Deleting an SNMPv3 Community Table Entry	255
Modifying an SNMPv3 Community Table Entry	255
Displaying SNMPv3 Tables	258
Displaying User Table Entries	259
Displaying View Table Entries	261
Displaying Access Table Entries	262
Displaying SecurityToGroup Table Entries	263
Displaying Notify Table Entries	264
Displaying Target Address Table Entries	265
Displaying Target Parameters Table Entries	266
Displaying SNMPv3 Community Table Entries	267

Section III

VLANs269

Chapter 17

Virtual LANs	271
Creating a New Port-Based or Tagged VLAN	272
Modifying a VLAN	276
Deleting a VLAN	278
Selecting a VLAN Mode	279
Displaying VLANs	281
Specifying a Management VLAN	283

Chapter 18

GARP VLAN Registration Protocol (GVRP)	285
Configuring GVRP	286
Enabling or Disabling GVRP on a Port	288
Displaying the GVRP Configuration	289

Displaying the GVRP Port Configuration	291
Displaying the GVRP Database	292
Displaying the GVRP State Machine	293
Displaying the GVRP Counters	296
Displaying the GIP Connected Ports Ring	300

Section IV

Security303

Chapter 19	
Port Security305	
Displaying the MAC Address Security Level	306

Chapter 20	
Encryption Keys, PKI, and SSL309	
Displaying the Encryption Keys	310
Displaying the PKI Settings and Certificates	312
Displaying the SSL Settings	315

Chapter 21	
Secure Shell (SSH)317	
Configuring SSH	318
Displaying the SSH Settings	320

Chapter 22	
TACACS+ and RADIUS323	
Enabling or Disabling TACACS+ or RADIUS	324
Configuring TACACS+	325
Displaying the TACACS+ Settings	327
Configuring RADIUS	329
Displaying the RADIUS Settings	331

Chapter 23	
802.1x Port-based Network Access Control333	
Setting Port Roles	334
Enabling or Disabling 802.1x Port-based Network Access Control	336
Configuring Authenticator Port Parameters	337
Configuring Supplicant Port Parameters	340
Displaying the Port-based Network Access Control Parameters	342
Displaying the Port Status	342
Displaying the Port Settings	343
RADIUS Accounting	346
Configuring RADIUS Accounting	346
Displaying the RADIUS Accounting Settings	347

Chapter 24	
Denial of Service Defense351	
Configuring Denial of Service Defense	352
Displaying the DoS Settings	355

Appendix A	
AT-S63 Default Settings357	
Basic Switch Default Settings	359
Boot Configuration File Default Setting	359
Management Access Default Settings	359
Management Interface Default Settings	359
RJ-45 Serial Terminal Port Default Settings	360
SNTP Default Settings	360

Switch Administration Default Settings	361
System Software Default Settings	361
Enhanced Stacking Default Setting	362
SNMP Default Settings	363
Port Configuration Default Settings	364
Event Log Default Settings	365
Quality of Service	366
IGMP Snooping Default Settings	367
Denial of Service Prevention Default Settings	368
STP, RSTP, and MSTP Default Settings	369
Spanning Tree Switch Settings	369
STP Default Settings	369
RSTP Default Settings	369
MSTP Default Settings	370
VLAN Default Settings	371
GVRP Default Settings	372
Port Security Default Settings	373
802.1x Port-Based Network Access Control Default Settings	374
Web Server Default Settings	375
SSL Default Settings	376
PKI Default Settings	377
SSH Default Settings	378
Server-Based Authentication Default Settings	379
Server-Based Authentication Default Settings	379
RADIUS Default Settings	379
TACACS+ Client Default Settings	379
Management Access Control List Default Setting	380
Index	381

Figures

Figure 1: Entering a Switch's IP Address in the URL Field	32
Figure 2: AT-S63 Login Page	33
Figure 3: Home page	34
Figure 4: Save Changes Button in the General Tab (Configuration)	36
Figure 5: General Tab (Configuration)	40
Figure 6: General Tab (Monitoring)	44
Figure 7: Ping Client Tab (Monitoring)	49
Figure 8: System Utilities Tab (Configuration)	51
Figure 9: SNMP Tab (Configuration)	54
Figure 10: SNMPv1 & SNMPv2c Communities Tab	56
Figure 11: Add New SNMPv1 & SNMPv2c Community Page	57
Figure 12: Modify SNMPv1 & SNMPv2c Community Page	59
Figure 13: SNMP Tab (Monitoring)	62
Figure 14: SNMPv1 & SNMPv2c Communities Tab (Monitoring)	63
Figure 15: Enhanced Stacking Tab (Configuration)	67
Figure 16: Stacking Switches Page	69
Figure 17: Enhanced Stacking Tab (Monitoring)	72
Figure 18: Port Settings Tab (Configuration)	74
Figure 19: Port Configuration Page	75
Figure 20: Port Settings Tab (Monitoring)	81
Figure 21: Port Status Page	82
Figure 22: Port Statistics Page	85
Figure 23: MAC Address Tab (Configuration)	90
Figure 24: Add MAC Address Page	91
Figure 25: MAC Address Tab (Monitoring)	94
Figure 26: View MAC Addresses Page	96
Figure 27: Port Trunking Tab (Configuration)	100
Figure 28: Add New Trunk Page	101
Figure 29: Modify Trunk Page	104
Figure 30: Port Trunking Tab (Monitoring)	106
Figure 31: Port Mirroring Tab (Configuration)	110
Figure 32: Modify Mirror Page	111
Figure 33: Example of a Modify Mirror Page	112
Figure 34: Port Mirroring Tab (Monitoring)	116
Figure 35: System Utilities Tab (Configuration)	123
Figure 36: Event Log Tab (Configuration)	128
Figure 37: Event Log Tab (Monitoring)	130

Figure 38: Event Log Example Displayed in Normal Mode	134
Figure 39: Event Log Example Displayed in Full Mode	135
Figure 40: CoS Tab (Configuration)	142
Figure 41: CoS Setting for Port Page	143
Figure 42: QoS Scheduling Tab (Configuration)	146
Figure 43: CoS Tab (Monitoring)	150
Figure 44: CoS Setting for Port Page	150
Figure 45: QoS Scheduling Tab (Monitoring)	152
Figure 46: IGMP Tab (Configuration)	154
Figure 47: IGMP Tab (Monitoring)	157
Figure 48: View Multicast Hosts List Page	158
Figure 49: View Multicast Routers List Page	160
Figure 50: View (Static) Multicast Routers List Page	161
Figure 51: Spanning Tree Tab (Configuration)	164
Figure 52: Configure STP Parameters Tab (Configuration)	167
Figure 53: STP Settings - Port(s) Page	169
Figure 54: Spanning Tree Tab (Monitoring)	171
Figure 55: Monitor STP Parameters Tab (Monitoring)	171
Figure 56: STP Settings Page	172
Figure 57: Configure RSTP Parameters Tab (Configuration)	175
Figure 58: RSTP Settings - Port(s) Page	177
Figure 59: Monitor RSTP Parameters Tab (Monitoring)	179
Figure 60: RSTP Settings Page	179
Figure 61: Spanning Tree Tab (Configuration)	182
Figure 62: Configure MSTP Parameters Tab (Configuration)	185
Figure 63: Add New MSTI Page	189
Figure 64: Modify MSTI Page	191
Figure 65: MSTP Settings - Port(s) Page	195
Figure 66: Monitor MSTP Parameters Tab (Monitoring)	198
Figure 67: MSTP Settings - Port(s) Page	198
Figure 68: MSTP Port Status - Port(s) Page	200
Figure 69: SNMP Tab (Configuration)	205
Figure 70: SNMPv3 User Table Tab (Configuration)	208
Figure 71: Add New SNMPv3 User Page	208
Figure 72: Modify SNMPv3 User Page	211
Figure 73: SNMPv3 View Table Tab (Configuration)	215
Figure 74: Add New SNMPv3 View Page	215
Figure 75: Modify SNMPv3 View Page	218
Figure 76: SNMPv3 Access Table Tab (Configuration)	221
Figure 77: Add New SNMPv3 Access Page	221
Figure 78: Modify SNMPv3 Access Page	225
Figure 79: SNMPv3 SecurityToGroup Table Tab (Configuration)	228
Figure 80: Add New SNMPv3 SecurityToGroup Page	228
Figure 81: Modify SNMPv3 SecurityToGroup Page	231
Figure 82: SNMPv3 Notify Table Tab (Configuration)	234
Figure 83: Add New SNMPv3 Notify Page	234
Figure 84: Modify SNMPv3 Notify Page	236
Figure 85: SNMPv3 Target Address Table Tab (Configuration)	239
Figure 86: Add New SNMPv3 Target Address Page	239
Figure 87: Modify SNMPv3 Target Address Page	242
Figure 88: SNMPv3 Target Parameters Table Tab (Configuration)	245
Figure 89: Add New SNMPv3 Target Parameters Page	246
Figure 90: Modify SNMPv3 Target Parameter Page	249
Figure 91: SNMPv3 Community Table Tab (Configuration)	253
Figure 92: Add New SNMPv3 Community Page	253

Figure 93: Modify SNMPv3 Community Page	256
Figure 94: SNMP Tab (Monitoring)	259
Figure 95: SNMPv3 User Table Tab (Monitoring)	260
Figure 96: SNMPv3 View Table Tab (Monitoring)	261
Figure 97: SNMPv3 Access Table Tab (Monitoring)	262
Figure 98: SNMPv3 SecurityToGroup Table Tab (Monitoring)	263
Figure 99: SNMPv3 Notify Table Tab (Monitoring)	264
Figure 100: SNMPv3 Target Address Table Tab (Monitoring)	265
Figure 101: SNMPv3 Target Parameters Table Tab (Monitoring)	266
Figure 102: SNMPv3 Community Table Tab (Monitoring)	267
Figure 103: VLAN Tab (Configuration)	272
Figure 104: Add New VLAN Page	273
Figure 105: VLAN Tab (Monitoring)	281
Figure 106: GVRP Tab (Configuration)	286
Figure 107: GVRP Port Configuration Page	288
Figure 108: GVRP Tab (Monitoring)	289
Figure 109: GVRP Port Configuration Page	291
Figure 110: GVRP Database Page	292
Figure 111: GVRP State Machine for VLAN Page	293
Figure 112: GVRP Counters Page	296
Figure 113: GIP Connected Ports Ring Page	300
Figure 114: Port Security Tab (Monitoring)	306
Figure 115: Security for Port(s) Page	307
Figure 116: 802.1x Port Access Tab (Monitoring)	310
Figure 117: Keys Tab (Monitoring)	311
Figure 118: PKI Tab (Monitoring)	312
Figure 119: X509 Certificate Details Page	313
Figure 120: SSL Tab (Monitoring)	315
Figure 121: Secure Shell Tab (Configuration)	318
Figure 122: Secure Shell Tab (Monitoring)	320
Figure 123: Server-based Authentication Tab (Configuration)	324
Figure 124: TACACS+ Client Configuration Page	325
Figure 125: Server-Based Authentication Tab (Monitoring)	327
Figure 126: TACACS+ Client Configuration Page	328
Figure 127: RADIUS Client Configuration Page	329
Figure 128: RADIUS Client Configuration Page	331
Figure 129: 802.1x Port Access Tab (Configuration)	334
Figure 130: Port Role Configuration Page	335
Figure 131: Authenticator Parameters Page	337
Figure 132: Supplicant Parameters Page	340
Figure 133: 802.1x Port Access Tab (Monitoring)	342
Figure 134: Port Access Port Status Page	343
Figure 135: Authenticator Port Parameters Page	344
Figure 136: Supplicant Port Parameters Page	345
Figure 137: 802.1x Port Access Tab (Configuration)	346
Figure 138: 802.1x Port Access Tab (Monitoring)	348
Figure 139: DoS Tab (Configuration)	352
Figure 140: DoS Configuration for Ports Page	353
Figure 141: DoS Tab (Monitoring)	355
Figure 142: DoS Monitor for Ports Page	356

Tables

Table 1: AT-S63 Software Modules	132
Table 2: Event Severity Levels	134
Table 3: Default Mappings of IEEE 802.1p Priority Levels to Priority Queues	143
Table 4: Example of Weighted Round Robin Priority	148
Table 5: Bridge Priority Value Increments	168
Table 6: Port Priority Value Increments	169
Table 7: GVRP State Machine Parameters	293
Table 8: GVRP Counters	297

Preface

This guide contains instructions on how to configure an AT-9400 Series Layer 2+ Gigabit Ethernet Switch using the AT-S63 management software and the web browser user interface.

How This Guide is Organized

This manual is divided into three sections.

Section I: Basic Features

The chapters in this section explain how to start a local management session and perform some basic tasks such as configuring switch and port parameters, port trunking, and enhanced stacking.

Section II: Advanced Features

The Advanced Features section includes procedures for working with the file system, spanning tree, IGMP, Quality of Service, the event log, and VLANs.

Section III: Security

The chapters in this section explain how to use a wide variety of switch security features including management ACLs, encryption, web server, port-based access control, denial of service defense, TACACS+, and RADIUS.

For information about managing an AT-9400 Series switch using the menus interface, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

To manage the switch using the command line interface, refer to the *AT-S63 Management Software Command Line Interface User's Guide*.



Caution

The software described in this documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a “retail encryption item” in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesyn sales representative for current information on this product’s export status.

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.



Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.



Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in portable document format (PDF) from on our web site at **www.alliedtelesyn.com**. You can view the documents online or download them onto a local workstation or server.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base at **www.alliedtelesyn.com/kb**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site, **www.alliedtelesyn.com**.

For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information at our web site: **www.alliedtelesyn.com**. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

New releases of management software for our managed products can be downloaded from either of the following Internet sites:

- ☐ Allied Telesyn web site: **www.alliedtelesyn.com**
- ☐ Allied Telesyn FTP server: **<ftp://ftp.alliedtelesyn.com>**

If you prefer to download new software from the Allied Telesyn FTP server using your workstation's command prompt, you need the FTP client software and you must log in to the server. Enter "anonymous" as the user name and your email address for the password.

Chapter 1

Overview

This chapter describes the AT-S63 software functions, the types of sessions you can use to access the software, and the management access levels. This chapter contains the following sections:

- ❑ "Management Overview" on page 22
- ❑ "Local Management Session" on page 24
- ❑ "Telnet Management Session" on page 25
- ❑ "Web Browser Management Session" on page 26
- ❑ "SNMP Management Session" on page 27
- ❑ "Management Access Levels" on page 28

Management Overview

The AT-S63 management software is intended for the AT-9400 Series switches. You use the software to monitor and adjust the switch's operating parameters. Some of the functions you can perform with the software include:

- ☐ Enable and disable ports
- ☐ Configure port parameters, such as speed and duplex mode
- ☐ Create virtual LANs (VLANs)
- ☐ Create port trunks and port mirrors
- ☐ Assign an Internet Protocol (IP) address and subnet mask
- ☐ Activate and configure the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), or Multiple Spanning Tree Protocol (MSTP)
- ☐ Activate enhanced stacking functions
- ☐ Configure Quality of Service (QoS)
- ☐ Enable and configure Internet Group Management Protocol (IGMP) snooping
- ☐ Download and upload image, configuration, and system files
- ☐ Configure port security

The AT-S63 management software is preinstalled on the switch with default settings for all operating parameters. If the default settings are adequate for your network, you can use the device as an unmanaged switch by connecting it to your network, as explained in the hardware installation guide, and powering on the switch.

Note

The default settings for the management software can be found in Appendix A, "AT-S63 Default Settings" on page 357.

To actively manage a switch by adjusting its operating parameters, you must access the AT-S63 management software. The AT-S63 management software provides a menu interface that makes it very easy to use (see the *AT-S63 Management Software Menu Interface User's Guide*), and an interface for managing a switch using a web browser (described in this guide). It also features a command line interface (see the *AT-S63 Management Software Command Line Interface User's Guide*).

There are four ways to access the management software on an AT-9400 Series switch. These methods are referred to in this guide as management sessions. They are:

- ☐ Local management session
- ☐ Telnet management session
- ☐ Web browser management session
- ☐ SNMP management session

The following sections in this chapter briefly describe each type of management session.

Local Management Session

You establish a local management session with an AT-9400 Series switch by connecting a terminal or a PC with a terminal emulator program to the terminal port on the switch, using the RJ-45 to RS-232 management cable included with the switch. The terminal port is located on the front panel of the AT-9400 Series switch.

This type of management session is referred to as “local” because you must be physically close to the switch, such as in the wiring closet where the switch is located.

After the session starts, a menu is displayed from which you can make selections to configure and monitor the switch. You can configure all of a switch’s operating parameters from a local management session using the menus or CLI interface.

Note

For instructions on starting a local management session, refer to Chapter 2, “Starting a Local or Telnet Management Session” in the *AT-S63 Management Software Menus Interface User’s Guide*.

A switch does not need an Internet Protocol (IP) address for you to manage it locally. You can start a local management session on a switch at any time. It does not affect the forwarding of frames by the device.

Assigning an AT-9400 Series switch an IP address and designating it as a master switch allows you to manage more than that switch. You can manage all of the switches that support enhanced stacking that reside in the same subnet, all from the same local management session.

Note

For further information on enhanced stacking, refer to Chapter 5, “Enhanced Stacking,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Telnet Management Session

You can use any management station on your network that has the Telnet application to manage an AT-9400 Series switch. This type of management session is referred to in this guide as a remote management session because you do not need to be in the wiring closet where the switch is located. You can manage the switch from any workstation on the network that has the application protocol.

To establish a Telnet management session with a switch, there must be at least one enhanced stacking switch in the subnet to which you assigned an IP address. Only one switch in a subnet needs to have an IP address. After you have established a Telnet management session with the switch that has an IP address, you can use the enhanced stacking feature of the management software to access all other switches that support enhanced stacking that reside in the same subnet.

Note

For further information on enhanced stacking, refer to Chapter 5, "Enhanced Stacking," in the *AT-S63 Management Software Menus Interface User's Guide*.

Note

For instructions on how to start a Telnet management session, refer to Chapter 2, "Starting a Local or Telnet Management Session" in the *AT-S63 Management Software Menus Interface User's Guide*.

A Telnet management session provides access to nearly all of a switch's operating parameters. You can perform nearly all the same functions from a Telnet management session as you can from a local management session.

Web Browser Management Session

You can also use a web browser to manage a switch. This too is referred to as remote management, just like a Telnet management session. You can manage a switch from any workstation on your network that has a web browser. It also uses the enhanced stacking feature. This means there needs to be just one switch on the subnet with an Internet Protocol (IP) address for you to be able to manage all the switches with a web browser. For instructions on starting this type of management session, refer to Chapter 2, "Starting a Web Browser Management Session" on page 31.

SNMP Management Session

Another way to remotely manage the switch is with an SNMP management program. A familiarity with using management information base (MIB) objects is necessary for this type of management.

The AT-S63 software supports the following MIBs:

- ☐ SNMP MIB-II (RFC 1213)
- ☐ Bridge MIB (RFC 1493)
- ☐ Interface Group MIB (RFC 1573)
- ☐ Ethernet MIB (RFC 1643)
- ☐ Remote Network MIB (RFC 1757)
- ☐ Allied Telesyn managed switch MIBs

You must download the Allied Telesyn managed switch MIBs (atistackinfo.mib and atiswitch.mib) file from the Allied Telesyn web site and compile the files with your SNMP program. For instructions, refer to your SNMP management documentation.

Note

SNMP management does not use the enhanced stacking feature of the switch. Therefore, you must assign an IP address to each switch that you want to manage with an SNMP program.

Management Access Levels

There are two levels of management access in the AT-S63 management software: manager and operator. When you log in as a manager, you can view and configure all of a switch's operating parameters. When you log in as an operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator by entering the appropriate username and password when you start an AT-S63 management session. To log in as a manager, type "manager" as the login name. The default password is "friend." The username for operator is "operator" and the default password is also "operator." The usernames and passwords are case sensitive.

To change the passwords, refer to "Configuring the Manager and Operator Passwords" on page 46.

Section I

Basic Features

The chapters in this section provide information and procedures for basic switch setup and include:

- ❑ Chapter 2, "Starting a Web Browser Management Session" on page 31
- ❑ Chapter 3, "Basic Switch Parameters" on page 39
- ❑ Chapter 4, "SNMPv1 and SNMPv2c" on page 53
- ❑ Chapter 5, "Enhanced Stacking" on page 65
- ❑ Chapter 6, "Port Parameters" on page 73
- ❑ Chapter 7, "MAC Address Table" on page 89
- ❑ Chapter 8, "Port Trunking" on page 99
- ❑ Chapter 9, "Port Mirroring" on page 109

Chapter 2

Starting a Web Browser Management Session

This chapter contains the procedure for starting, saving, and quitting a web browser management session on an AT-9400 Series switch. Sections in the chapter include:

- ❑ "Starting a Web Browser Management Session" on page 32
- ❑ "Web Browser Tools" on page 35
- ❑ "Saving Your Parameter Changes" on page 36
- ❑ "Quitting a Web Browser Management Session" on page 37

Starting a Web Browser Management Session

To establish a web browser management session with an AT-9400 Series switch, there must be at least one switch in the subnet that has been assigned an IP address and whose stacking status has been changed to master switch. After you start a web browser management session on the master switch, you can manage all the enhanced stacking switches that reside in the same subnet.

If the subnet does not contain an enhanced stacking switch with an IP address, then you must use the menus or the command line interface (CLI) to give the switch an IP address and subnet mask. Then you can connect to that switch and start a web browser management session.

Note

For background information on enhanced stacking, refer to Chapter 5, "Enhanced Stacking," in the *AT-S63 Management Software Menus Interface User's Guide*.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

Note

If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser's network options not to use proxies. Consult your web browser's documentation on how to configure the switch's web browser not to use proxies.

2. In the URL field of the browser, enter the IP address of the switch you want to manage or of the master switch of the enhanced stack.

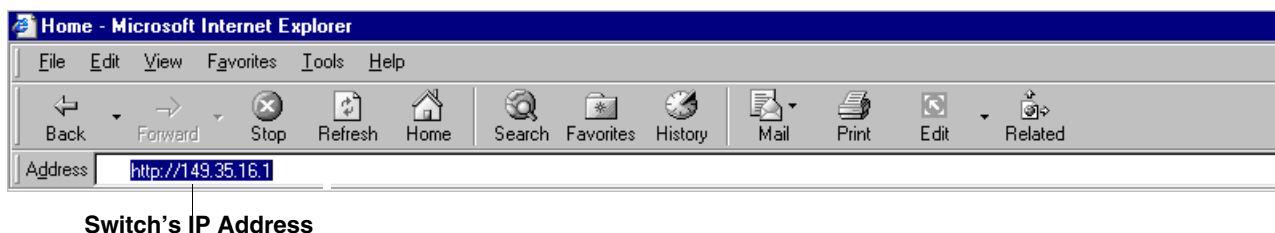


Figure 1. Entering a Switch's IP Address in the URL Field

The AT-S63 management software displays the login page, as shown in Figure 2.

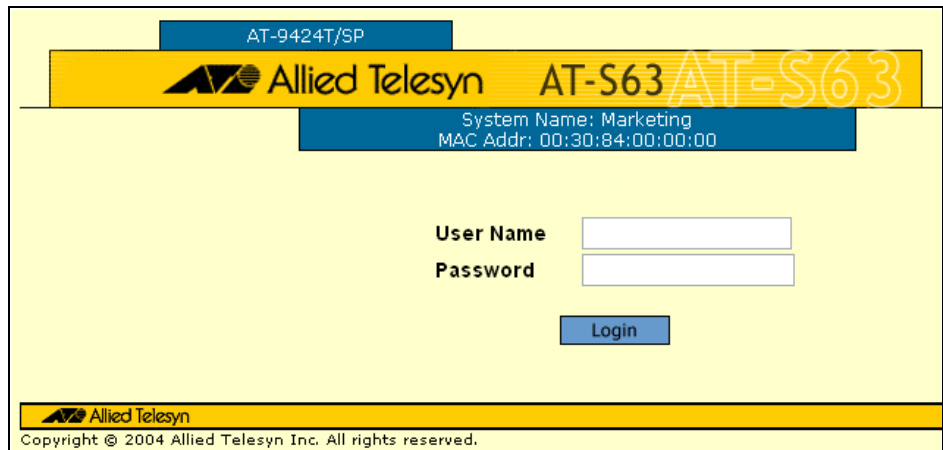


Figure 2. AT-S63 Login Page

3. Enter a user name and password. For manager access, enter "manager" as the user name. The default password is "friend." For operator access, enter "operator" as the user name. The default password is "operator." Login names and passwords are case-sensitive. (For information on the two access levels, refer to "Management Access" in Chapter 1, "Overview," of the *AT-S63 Management Software Menus Interface User's Guide*.)

You cannot change the user names. To change a password, refer to "Configuring the Manager and Operator Passwords" on page 46.

The home page is shown in Figure 3.

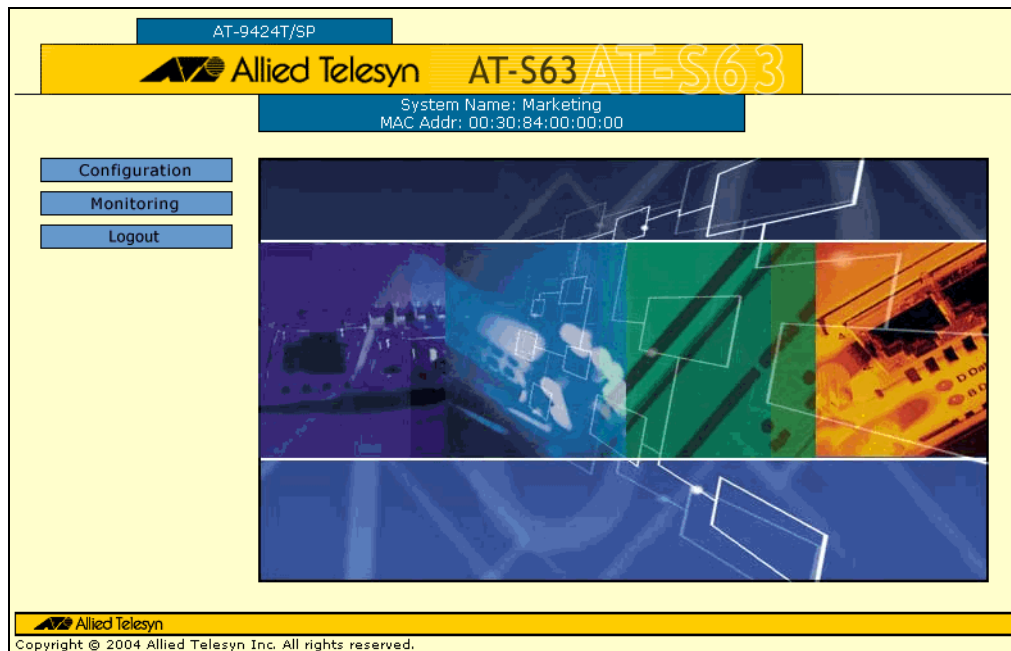


Figure 3. Home page

The main menu is on the left side of the home page. It consists of the following selections:

- ☐ Enhanced Stacking
- ☐ Configuration
- ☐ Monitoring
- ☐ Logout

Note

The Enhanced Stacking selection is included in the menu only if the switch is a master switch.

A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit the browser.

Web Browser Tools

You can use the web browser tools to move around the management pages. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature to save the link to the switch.

Saving Your Parameter Changes

When you make a change to a switch parameter, the change is, in most cases, immediately activated as soon as you click the Apply button on the page. However, a change to a switch parameter is initially saved only to temporary memory. It is lost the next time you reset or power cycle the unit. To permanently save a change, you must click the **Save Changes** button. This button is located on the General tab.

To locate the button, from the home page click Configuration. The General tab is displayed. The Save Changes button is at the bottom of the page. If the button is not displayed, there are no changes for the switch to save.

The screenshot shows the Configuration page for a switch (AT-9424T/SP). The page has a yellow background and a blue header. The header displays the System Name: Marketing and MAC Addr: 00:30:84:AB:EF:CD. The left sidebar contains navigation buttons: Home, System, Layer 1, Layer 2, Security, QoS, Help, and Logout. The main content area has tabs for General, SNMP, IGMP, System Utilities, Server-based Authentication, and Event Log. The General tab is active, showing the Administration section with fields for System Name (Marketing), Administrator (Josh), and Comments. The Passwords section has fields for Manager Password, Confirm Manager Password, Operator Password, and Confirm Operator Password. The Configuration section has a BOOTP/DHCP section with radio buttons for Enable (selected) and Disable, and a MAC Address Aging Time section with a text box containing 300 and the label second(s). At the bottom of the page, there are four buttons: Apply, Defaults, Save Changes, and Reset. A line points from the text 'Save Changes Button' to the Save Changes button.

Figure 4. Save Changes Button in the General Tab (Configuration)

Quitting a Web Browser Management Session

To exit a web browser management session, select the **Logout** option from the main menu.

Chapter 3

Basic Switch Parameters

This chapter contains the following sections:

- ❑ "Configuring an IP Address and Switch Name" on page 40
- ❑ "Activating the BOOTP and DHCP Client Software" on page 43
- ❑ "Displaying System Information" on page 44
- ❑ "Configuring the Manager and Operator Passwords" on page 46
- ❑ "Rebooting a Switch" on page 48
- ❑ "Pinging a Remote System" on page 49
- ❑ "Returning the AT-S63 Management Software to the Factory Default Values" on page 50

Configuring an IP Address and Switch Name

Note
For guidelines about when to assign an IP address, subnet address, and gateway address to an AT-9400 Series switch, refer to “When Does a Switch Need an IP Address?” in Chapter 3, “Basic Switch Parameters,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

To set basic switch parameters for an AT-9400 Series switch, perform the following procedure:

- 1. From the home page, select **Configuration**.
The System page is displayed with the General tab selected by default, as shown in Figure 5.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Home
System
Layer 1
Layer 2
Security
QoS
Help
Logout

GeneralSNMPIGMPSystem UtilitiesServer-based AuthenticationEvent Log

Administration

System Name
Marketing

Administrator

Comments

IP Address
149.35.19.172

Subnet Mask
255.255.252.0

Default Gateway
149.35.16.1

Passwords

Manager Password

Confirm Manager Password

Operator Password

Confirm Operator Password

Configuration

BOOTP/DHCP
Enable Disable

MAC Address Aging Time
300 second(s)

ApplyDefaultsReset

Figure 5. General Tab (Configuration)

Note

This procedure describes the parameters in the Administration section of the tab. The Passwords section is described in "Configuring the Manager and Operator Passwords" on page 46. The DHCP/BOOTP option is described in "Activating the BOOTP and DHCP Client Software" on page 43. The maximum aging timer option is described in "Changing the Aging Time" on page 97.

Note

The Defaults button returns all parameters in this tab to their default settings. The Reset button resets the switch. For instructions, refer to "Rebooting a Switch" on page 48.

2. Adjust the following parameters as necessary:

System Name

This parameter specifies a name for the switch (for example, Sales Ethernet switch). The name is displayed at the top of the AT-S63 management pages and tabs. The name can be from 1 to 39 characters. The name can include spaces and special characters, such as exclamation points and asterisks. The default is no name. This parameter is optional.

Note

Allied Telesyn recommends assigning each switch a name. Names make it easier for you to identify the various switches when you manage them, and they can help you avoid performing a configuration procedure on the wrong switch.

Administrator

This parameter specifies the name of the network administrator responsible for managing the switch. The name can be from 1 to 20 characters. It can include spaces and special characters, such as dashes and asterisks. The default is no name. This parameter is optional.

Comments

This parameter specifies the location of the switch, (for example, 4th Floor - rm 402B). The location can be from 1 to 20 characters. The location can include spaces and special characters, such as dashes and asterisks. The default is no location. This parameter is optional.

IP Address

This parameter specifies the IP address of the switch. You must specify an IP address if you want the switch to function as the Master switch of an enhanced stack. The IP address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

Subnet Mask

This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch. The subnet mask must be entered in the format: xxx.xxx.xxx.xxx. The default value is 255.255.0.0.

Default Gateway

This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router. The address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

3. Click **Apply** to activate your changes on the switch.

Note

A change to any of the above parameters is immediately activated on the switch.

A change to the IP address of the switch results in the loss of a remote management session. You can restart the management session using the switch's new IP address.

4. Click **Save Changes** to permanently save your changes. (This button is not displayed if there are no changes to save.)

Activating the BOOTP and DHCP Client Software

For background information on BOOTP and DHCP, refer to Chapter 3, "Basic Switch Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

To activate or deactivate the BOOTP and DHCP client software on the switch from a web browser management session, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. In the BOOTP/DHCP section, click either **Enable** to activate the client software or **Disable** to disable it. The default is disabled.
3. Click **Apply** to activate your change on the switch.

Note

If you activated BOOTP/DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response. If you manually assigned the switch and IP address, that address is deleted and replaced by the IP address received from the BOOTP/DHCP server.

4. Click **Save Changes** to permanently save your changes. (This button is not displayed if there are no changes to save.)

Displaying System Information

To view basic information about the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6.

The screenshot shows the 'Monitoring' page for switch 'AT-9424T/SP'. The 'General' tab is selected. The interface includes a sidebar with navigation links (Home, System, Layer 1, Layer 2, Security, QoS, Help, Logout) and a main content area with several sections: General, System Software, Hardware, and Voltage.

General

System Name Marketing	IP Address 149.35.19.158
Administrator Joe B.	Subnet Mask 255.255.252.0
Comments 3rd Floor	Default Gateway 149.35.16.1
BOOTP/DHCP Enabled	
MAC Address Aging Time 300 second(s)	System Up Time 52 Days 0 Hours 25 Minutes 12 Seconds

System Software

Application Software	AT863 v1.0.0 (Mar 12 2004 15:43:53)
Bootloader	AT863_LOADER v1.0.0 (Feb 12 2004 10:52:33)

Hardware

Model Name	Serial Number	Temperature (Deg. C)	Upper Temp. Threshold (Deg. C)	Fan 1 Speed RPM	Fan 2 Speed RPM
AT-9424T/SP	S05525A023600001	36	90	3970	Off

Voltage

2.5 V	3.3 V	5.0 V	1.8 V	1.25 V	12.0 V
2.48	3.30	5.04	1.76	1.28	11.68

Figure 6. General Tab (Monitoring)

The General section displays the following information:

System Name

The name of the switch.

Administrator

The name of the network administrator responsible for managing the switch.

Comments

The location of the switch, (for example, 4th Floor - rm 402B).

DHCP/BOOTP

The status of the DHCP and BOOTP client software. If enabled, the switch is obtaining its IP information from a DHCP and BOOTP server on the network. If disabled, the IP address must be manually entered.

MAC Address Aging Timer

The time interval an inactive dynamic MAC address can remain in the MAC address table before it is deleted.

IP Address

The switch's IP address.

Subnet Mask

The switch's subnet mask.

Default Gateway

The IP address of a router for remote management.

System Up Time

The length of time since the switch was last reset or power cycled.

The System Software section displays the following information:

Application Software

The version number and build date of the AT-S63 management software.

Bootloader

The version number and build date of the AT-S63 bootloader.

The Hardware section displays the following information:

Model Name

The model name.

Serial Number

The switch serial number.

Temperature (Deg.C)

The current system temperature.

Upper Temp. Threshold (Deg C)

The upper threshold for the switch temperature.

Fan 1 Speed RPM**Fan 2 Speed RPM**

The speed of the system fan(s).

The Voltage section provides the current voltage of the six power supplies in the switch, identified as 2.5 V, 3.3 V, 5 V, 1.8 V, 1.25 V, and 12 V.

Configuring the Manager and Operator Passwords

There are two levels of management access on an AT-9400 Series switch: manager and operator. When you log in as a manager, you can view and configure all of a switch's operating parameters. When you log in as an operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator by entering the appropriate username and password when you start an AT-S63 management session. The default password for manager access is "friend." The default password for operator access is "operator." Passwords are case sensitive.

To change the manager or operator password, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. In the Passwords section, enter the new values. The parameters are described below.

Manager Password

Confirm Manager Password

You use these parameters to change the manager's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password is "friend." The password is case sensitive.



Caution

Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

Operator Password

Confirm Operator Password

Use these parameters to change the operator's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password for operator is "operator." The password is case sensitive.



Caution

Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

Note

A change to a password is immediately activated on the switch. You are prompted for the new password the next time you log in.

3. Click **Apply** to activate your change on the switch.
4. Click **Save Changes** to permanently save your change. (This button is not displayed if there are no changes to save.)

Rebooting a Switch

Note

Any parameters changes that have not been saved are discarded when a system is reset. To save parameter changes, refer to "Saving Your Parameter Changes" on page 36.

To reboot a switch, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Click **Reset**.

A confirmation prompt is displayed.

3. Click **OK** to reset the switch or **Cancel** to cancel the procedure:

Note

The switch does not forward packets while it reloads the AT-S63 management software, a process that takes approximately 20 seconds to complete.

Resetting the switch ends your web browser management session. You must restart the session to continue managing the switch.

Pinging a Remote System

You can instruct the switch to ping a node on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **Ping Client** tab.

The Ping Client tab is shown in Figure 7.

The screenshot shows the AT-S63 Management Software Web Browser Interface. At the top, there is a header bar with the text "AT-9424T/SP" and a large yellow banner with the word "Monitoring" in bold. Below the banner, there is a blue bar containing the text "System Name: Marketing" and "MAC Addr: 00:30:84:00:00:00". On the left side, there is a vertical menu with buttons for "Home", "System", "Layer 1", "Layer 2", "Security", "QoS", "Help", and "Logout". In the center, there are several tabs: "General", "SNMP", "IGMP", "Ping Client", "Server-based Authentication", and "Event Log". The "Ping Client" tab is currently selected. Below the tabs, there is a form with the label "IP Address:" followed by four input fields for the IP address (each with a dot separator) and an "OK" button.

Figure 7. Ping Client Tab (Monitoring)

3. Enter the IP address of the end node you want the switch to ping.
4. Click **OK**.

The results of the ping are displayed in a popup window.

5. To stop the ping, click **OK**.

Returning the AT-S63 Management Software to the Factory Default Values

The procedure in this section returns all AT-S63 management software parameters to their default values. Please note the following before you perform this procedure:

- ❑ Returning all parameter settings to their default values also deletes any port-based or tagged VLANs you created on the switch.
- ❑ This procedure does not delete files from the AT-S63 file system. To delete files, refer to Chapter 10, "File System," in the *AT-S63 Management Software Menus Interface User's Guide*.
- ❑ This procedure does not delete any encryption keys stored in the key database. To delete encryption keys, refer to "Deleting a Key," in Chapter 26, "Encryption Keys," in the *AT-S63 Management Software Menus Interface User's Guide*.
- ❑ Returning a switch to its default values deletes all configuration commands in the active boot configuration file. If you want to keep the file, you should either create a copy of it, as explained in Chapter 10, "File System," in the *AT-S63 Management Software Menus Interface User's Guide*. Or, you can assign another configuration file, one whose configuration you do not want to retain, as the active boot configuration file. The latter procedure is described in the same chapter.

Note

The AT-S63 management software default values are listed in Appendix A, "AT-S63 Default Settings" on page 357.

To return the AT-S63 management software to the default settings, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **System Utilities** tab.

The System Utilities tab is shown in Figure 8.

The screenshot displays the AT-S63 Management Software Web Browser Interface. At the top, a blue header bar shows 'AT-9424T/SP'. Below it, a yellow banner reads 'Configuration'. A blue box contains 'System Name: Marketing' and 'MAC Addr: 00:30:84:AB:EF:CD'. On the left, a vertical menu lists: Home, System, Layer 1, Layer 2, Security, QoS, Help, and Logout. The main content area has tabs: General, SNMP, IGMP, System Utilities (selected), Server-based Authentication, and Event Log. Under the 'System Utilities' tab, there is a checkbox labeled 'Reboot Switch After Resetting to Defaults'. Below this is an 'Apply' button. Further down, a section titled 'TFTP File Uploads and Downloads' contains two columns. The left column has 'TFTP Server IP Address' (four input boxes with '0'), 'TFTP Remote Filename' (text input), and 'TFTP FileType' (radio buttons for Image, Default Config, and General). The right column has 'TFTP Operation' (radio buttons for Download and Upload) and 'TFTP Local Filename' (text input). An 'Apply' button is at the bottom right of this section.

Figure 8. System Utilities Tab (Configuration)

3. Click the **Reboot Switch After Setting Defaults** checkbox.
4. Click **Apply**.

The web browser displays the following prompt:

This page may no longer be available while the switch reboots. Do you want to continue?

5. Click **OK** to continue, or **Cancel** to cancel the procedure:

Chapter 4

SNMPv1 and SNMPv2c

This chapter explains how to activate SNMP management on the switch and how to create, modify, and delete SNMPv1 and SNMPv2c community strings. This chapter contains the following procedures:

- ❑ "Enabling or Disabling SNMP Management" on page 54
- ❑ "Creating a New SNMPv1 and SNMPv2c Community" on page 56
- ❑ "Modifying an SNMPv1 and SNMPv2c Community" on page 59
- ❑ "Deleting an SNMPv1 and SNMPv2c Community" on page 61
- ❑ "Displaying the SNMPv1 and SNMPv2c Communities" on page 62

Note

For background information about SNMPv1 and SNMPv2c, refer to Chapter 4, "SNMPv1 and SNMPv2c," in the *AT-S63 Management Software Menus Interface User's Guide*.

Enabling or Disabling SNMP Management

To enable or disable SNMP management on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 9.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Home System Layer 1 Layer 2 Security QoS Help Logout

General **SNMP** IGMP System Utilities Server-based Authentication Event Log

☐ Enable SNMP Access
☐ Enable Authentication Failure Trap
Apply

SNMPv1/v2c
Configure SNMPv1/v2c Communities
Configure

SNMPv3
SNMP Engine ID : 80:00:00:CF:03:00:30:84:AB:EF:CD
☒ Configure User Table
☐ Configure View Table
☐ Configure Access Table
☐ Configure SecurityToGroup Table
☐ Configure Notify Table
☐ Configure Target Address Table
☐ Configure Target Parameters Table
☐ Configure Community Table
 Configure

Figure 9. SNMP Tab (Configuration)

3. Click the **Enable SNMP Access** checkbox to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the switch can be managed from an SNMP management station. No check indicates that the feature is disabled. The default is disabled.
4. If you want the switch to send authentication failure traps, click the **Enable Authentication Failure Traps** checkbox. A check in the box indicates that the switch sends the trap.

5. Click **Apply**.

A change to SNMP access is immediately activated on the switch.

The community strings that already exist on the switch are displayed in a table.

6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

Creating a New SNMPv1 and SNMPv2c Community

To create a new SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 9 on page 54.

3. In the SNMPv1 & SNMPv2c section, click **Configure**.

The SNMPv1 & SNMPv2c Communities tab is shown in Figure 10.

The screenshot shows the Configuration page for a device (AT-9424T/SP). The main heading is "Configuration". Below it, the System Name is "Marketing" and the MAC Address is "00:30:84:00:00:00". The left sidebar contains navigation links: Home, System, Layer 1, Layer 2, Security, QoS, Help, and Logout. The main content area has tabs for General, SNMP, IGMP, System Utilities, Server-based Authentication, and Event Log. The "SNMP" tab is selected, and the "SNMPv1 & SNMPv2c Communities" section is active. It shows a table with 3 entries and buttons for Refresh, Add, Remove, Modify, and Back.

Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status
<input checked="" type="radio"/> lemondrop19	Read Only			Yes	Enabled
<input type="radio"/> rootbeer14	Read Only	198.1.1.9	198.1.1.9	No	Enabled
<input type="radio"/> sassafras12	Read/Write	198.1.1.1, 198.20.2.2, 198.30.3.3	198.1.1.1, 198.20.2.2, 198.30.3.3	No	Enabled

Figure 10. SNMPv1 & SNMPv2c Communities Tab

4. Click **Add**.

The Add New SNMPv1 & SNMPv2c Community page is shown in Figure 11.

Add New SNMPv1 & SNMPv2c Community

Community Name :

Status : ☒ Enable ☐ Disable

Access Mode : ☒ Read Only ☐ Read-Write

Managers	Trap Receivers
<input type="checkbox"/> Allow Any Station	Trap Receiver IP Address 1 <input type="text"/>
Manager IP Address 1 <input type="text"/>	Trap Receiver IP Address 2 <input type="text"/>
Manager IP Address 2 <input type="text"/>	Trap Receiver IP Address 3 <input type="text"/>
Manager IP Address 3 <input type="text"/>	Trap Receiver IP Address 4 <input type="text"/>
Manager IP Address 4 <input type="text"/>	Trap Receiver IP Address 5 <input type="text"/>
Manager IP Address 5 <input type="text"/>	Trap Receiver IP Address 6 <input type="text"/>
Manager IP Address 6 <input type="text"/>	Trap Receiver IP Address 7 <input type="text"/>
Manager IP Address 7 <input type="text"/>	Trap Receiver IP Address 8 <input type="text"/>
Manager IP Address 8 <input type="text"/>	

Apply Cancel

Figure 11. Add New SNMPv1 & SNMPv2c Community Page

- Configure the following parameters:

Community Name

Enter an SNMP community name that consists of up to 15 alphanumeric characters.

Status

Click Enable to enable the SNMP community. Click Disable to disable the SNMP community.

Access Mode

Click Read Only to allow read access to the SNMP community. To allow read-write access to the SNMP community, click Read-Write.

Allow Any Station

Click this option to allow any SNMP manager to access the switch. When you click this option, a warning message appears on the screen. Click OK to continue.

Manager IP Address1 through **Manager IP Address 8**

Enter an IP Address of a switch that is permitted SNMP manager access to the current switch. You can enter up to 8 Manager IP Addresses.

Trap Receiver IP Address 1 through **Trap Receiver IP Address 8**

Use the above selections to specify the IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

6. Click **Apply**.
7. To save your changes, return to the General tab and click **Save Changes**.

Modifying an SNMPv1 and SNMPv2c Community

To modify an SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 9 on page 54.

3. In the SNMPv1 & SNMPv2c section, click **Configure**.

The SNMPv1 & SNMPv2c Communities tab is shown in Figure 10 on page 56.

4. Click the button next to the community name and click **Modify**.

The Modify SNMPv1 & SNMPv2c Community page is shown in Figure 12.

Figure 12. Modify SNMPv1 & SNMPv2c Community Page

5. Modify the following parameters:

Community Name

This field is not configurable from this page. It is the name of the SNMP community.

Status

Click Enable to enable the SNMP community. Click Disable to disable the SNMP community.

Access Mode

Click Read Only to allow read access to the SNMP community. Click Read-Write to allow read-write access to the SNMP community.

Allow Any Station

Click this option to allow any SNMP manager to access the switch. When you click this option, a warning message appears on the screen. Click OK to continue.

Manager IP Address 1 through **Manager IP Address 8**

Enter an IP Address of a switch that is permitted SNMP manager access to the current switch. You can enter up to 8 Manager IP Addresses.

Trap Receiver IP Address 1 through **Trap Receiver IP Address 8**

Use the above selections to specify the IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

6. Click **Apply**.
7. To save your changes, return to the General tab and click **Save Changes**.

Deleting an SNMPv1 and SNMPv2c Community

To delete an existing SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 9 on page 54.

3. In the SNMPv1 & SNMPv2c section, click **Configure**.

The SNMPv1 & SNMPv2c Communities tab is shown in Figure 10 on page 56.

4. Click the button next to the community name and click **Remove**.

A warning message is displayed.

5. Click **OK**.

6. To save your changes, return to the General tab and click **Save Changes**.

Displaying the SNMPv1 and SNMPv2c Communities

To display the SNMPv1 and SNMPv2c communities, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 13.

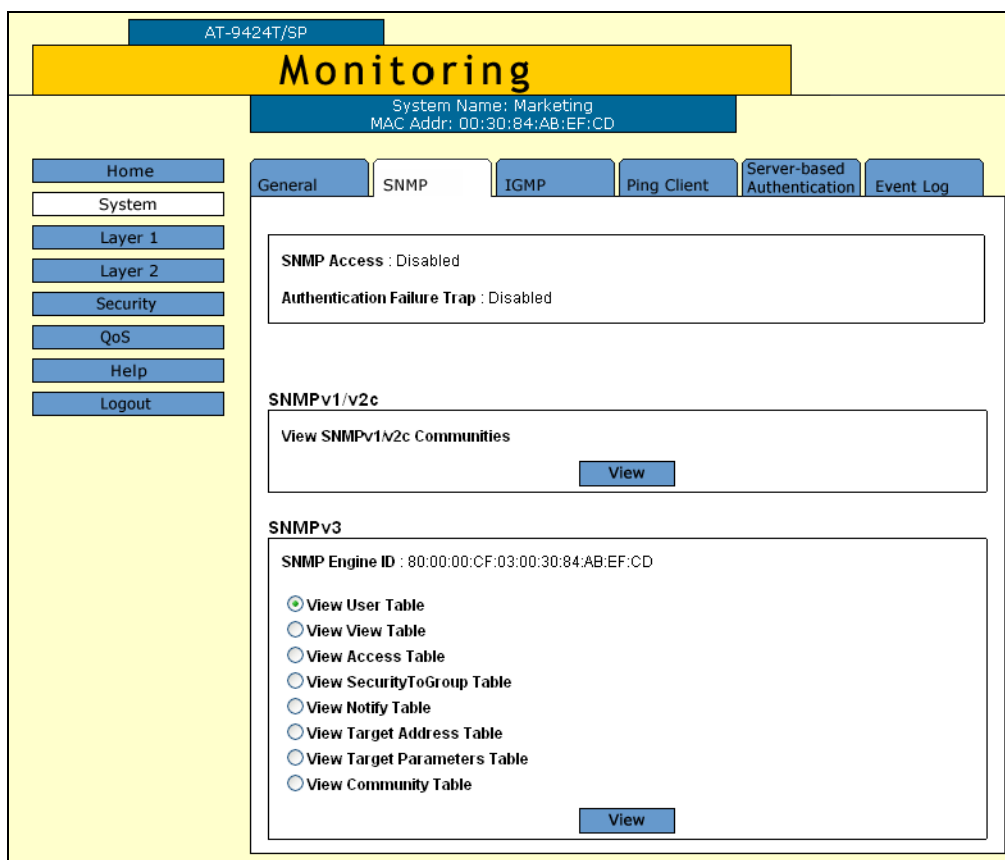


Figure 13. SNMP Tab (Monitoring)

3. In the SNMPv1 & SNMPv2c section, click **View**.

The SNMPv1 & SNMPv2c Communities tab is shown in Figure 14.

The screenshot shows the AT-S63 Management Software Web Browser Interface. The top status bar displays "AT-9424T/SP" and "Monitoring". Below the status bar, the system name is "Marketing" and the MAC address is "00:30:84:00:00:00". The navigation menu on the left includes links for Home, System, Layer 1, Layer 2, Security, QoS, Help, and Logout. The main content area shows the "SNMP" sub-tab, which displays the status of SNMP access and authentication failure traps. Below this, the "SNMPv1 & SNMPv2c Communities" table is shown, listing three communities: lemondrop19, rootbeer14, and sassafra12. The table includes columns for Community Name, Access Mode, Manager Stations, Trap Receivers, Open Access, and Status. The "Refresh" and "Back" buttons are located at the bottom of the table.

Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status
lemondrop19	Read Only	198.1.1.9	198.1.1.9	Yes	Enabled
rootbeer14	Read Only	198.1.1.1, 198.20.2.2, 198.30.3.3, 198.30.3.9	198.1.1.1, 198.20.2.2, 198.30.3.3, 198.30.3.9	No	Enabled
sassafra12	Read/Write	198.1.1.9	198.1.1.9	No	Enabled

Figure 14. SNMPv1 & SNMPv2c Communities Tab (Monitoring)

The SNMPv1 & SNMPv2c Communities tab displays a table that contains the following columns of information:

Community Name

The SNMP community name.

Access Mode

The access mode for access to that community. The possible settings are Read Only and Read/Write.

Manager Stations

The IP addresses of the management stations that are allowed SNMP access to the switch.

Trap Receivers

The IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

Open Access

The status of access to the SNMP community by a management station, one of the following settings:

Yes - Any management station can access the SNMP community.

No - Access to the SNMP community is only available to a management station configured within this community.

Status

The community status, one of the following settings:

Enabled - The community is enabled.

Disabled - The community is disabled.

Chapter 5

Enhanced Stacking

This chapter contains the following procedures for setting up enhanced stacking:

- ❑ "Setting a Switch's Enhanced Stacking Status" on page 66
- ❑ "Selecting a Switch in an Enhanced Stack" on page 68
- ❑ "Returning to the Master Switch" on page 71
- ❑ "Displaying the Enhanced Stacking Status" on page 72

Note

For background information on enhanced stacking, refer to Chapter 5, "Enhanced Stacking," in the *AT-S63 Management Software Menus Interface User's Guide*.

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master, slave, or unavailable. Each status is described below:

- ❑ **Master** - A master switch of a stack can be used to manage other enhanced stacking switches in a subnet. After you have established a local or remote management session with the master switch, you can access and manage the other enhanced stacking switches in the subnet.

A master switch must have a unique IP address. You can manually assign a master switch an IP address or activate the BOOTP and DHCP client software on the switch so that the switch automatically obtains an IP address from a BOOTP or DHCP server on your network.

- ❑ **Slave** - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask.
- ❑ **Unavailable** - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally. To be managed remotely, a switch with an unavailable stacking status must be assigned a unique IP address.

Note

The default setting for a switch is slave.

To adjust a switch's enhanced stacking status, perform the following procedure:

1. From the Home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Enhanced Stacking** tab.

The Enhanced Stacking tab is shown in Figure 15.

The screenshot displays the 'Configuration' page for an AT-9424T/SP switch. The system name is 'Marketing' and the MAC address is '00:30:84:00:00:00'. The left sidebar contains navigation links: Home, System, Layer 1, Layer 2, Security, QoS, Help, and Logout. The main content area has tabs for MAC Address, VLAN, GVRP, Spanning Tree, and Enhanced Stacking. The 'Enhanced Stacking' tab is active, showing a 'Switch State' section with three radio buttons: Master (selected), Slave, and Unavailable. An 'Apply' button is located below the radio buttons.

Figure 15. Enhanced Stacking Tab (Configuration)

4. Click the desired enhanced stacking status for the switch. The default is Slave.
5. Click **Apply**.

The new enhanced stacking status is immediately activated on the switch.

6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Selecting a Switch in an Enhanced Stack

Before you perform any procedure on a switch in an enhanced stack, check to be sure that you are performing it on the correct switch. If you assigned system names to your switches, identifying your switches is easy. The AT-S63 management software displays the name of the switch being managed at the top of every management menu.

When you start a web browser management session on the master switch of the enhanced stack, you are by default addressing that particular switch. The management tasks that you perform affect only the master switch.

To manage a slave switch or another master switch in the same stack, you need to select it from the management software.

To select a switch to manage in an enhanced stack, perform the following procedure:

1. From the home page, select **Enhanced Stacking**.

Note

If the Home page does not have an Enhanced Stacking menu option, the switch's enhanced stacking status is either slave or unavailable. For instructions on how to change a switch's stacking status, refer to the previous procedure:

The master switch polls the network for the slave and master enhanced stacking switches in the subnet and displays a list of the switches in the Stacking Switches page. An example is shown in Figure 16.

AT-9424T/SP

Enhanced Stacking

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home
Help
Logout

Stacking Switches

Total Switches: 12. Page 1 of 2

	No.	Mac Addr	Name	Switch Mode	Software Version	Switch Model
<input checked="" type="radio"/>	1	00:00:00:AA:BB:CD		Slave	S39 v3.2.0	AT-8012M
<input type="radio"/>	2	00:30:80:00:AD:34		Slave	S39 v3.1.1	AT-8012M
<input type="radio"/>	3	00:30:84:52:02:60	SV_USERS_8	Slave	S39 v3.1.1	AT-8024GB
<input type="radio"/>	4	00:30:84:54:AB:00		Slave	S39 v3.2.0 Pat	AT-8024GB
<input type="radio"/>	5	00:30:84:54:F5:80		Slave	S39 v3.2.0	AT-8024GB
<input type="radio"/>	6	00:30:84:F3:B4:00	SV_USERS_4	Slave	S39 v3.2.0	AT-8026T
<input type="radio"/>	7	00:30:84:F3:B4:20	SV_USERS_2	Slave	S39 v3.2.0	AT-8026T
<input type="radio"/>	8	00:30:84:F3:B5:00	SV_USERS_5	Slave	S39 v3.2.0	AT-8026T
<input type="radio"/>	9	00:30:84:F3:B6:20	SV_USERS_3	Slave	S39 v3.2.0	AT-8026T
<input type="radio"/>	10	00:30:84:F3:C9:40	SV_USERS_7	Slave	S39 v3.2.0	AT-8026T

Refresh Connect Next

Figure 16. Stacking Switches Page

Note

The master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of Unavailable.

You can sort the switches in the list by switch name or MAC address by clicking on the column headers. By default, the list is sorted by MAC address.

To refresh the list, click **Refresh**. This instructs the master switch to again poll the subnet for all switches.

2. To manage another switch in an enhanced stack, click the button to the left of the appropriate switch in the list. You can select only one switch at a time.

Note

If the web server on the master switch is operating in the secure HTTPS mode, you can manage only those enhanced stacking switches that are also operating HTTPS. You cannot manage a switch whose web server is operating in the non-secure HTTP mode.

3. Click **Connect**.

4. Enter a user name and password for the switch when prompted.

The home page of the selected switch is displayed. You can now manage the switch.

Returning to the Master Switch

When you are finished managing a slave switch and want to manage another switch in the stack, return to the Home page of the switch and select **Disconnect** from the menu. This returns you to the Enhanced Stacking page in Figure 16 on page 69. When you see that page, you are again addressing the master switch from which you started the management session.

You can select another switch in the list to manage or, if you want to manage the master switch, select **Home** to return to the master switch's home page.

Displaying the Enhanced Stacking Status

To display the enhanced stacking status of the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Layer 2**.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. From the Layer 2 page, select the **Enhanced Stacking** tab.

The Enhanced Stacking tab is shown Figure 17.

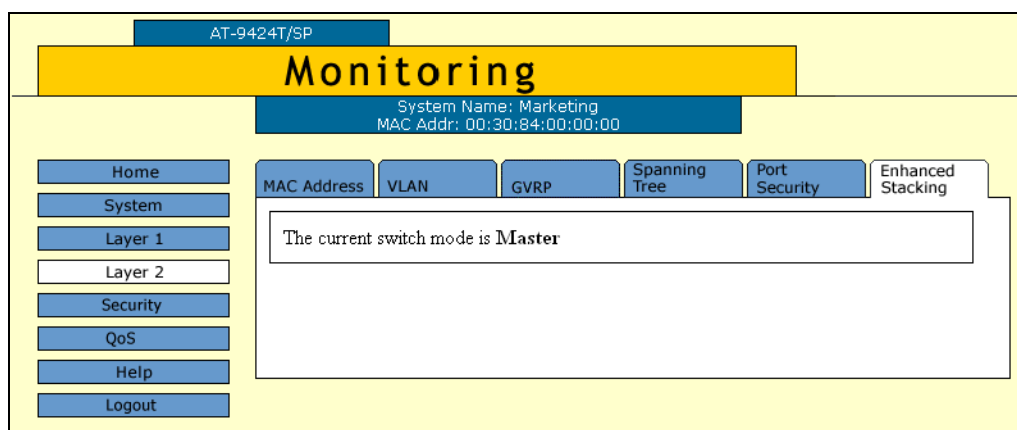


Figure 17. Enhanced Stacking Tab (Monitoring)

The information in the tab states the current enhanced stacking status of the switch as master, slave, or unavailable.

Chapter 6

Port Parameters

This chapter explains how to view and change the parameter settings for the individual ports on a switch. Examples of the parameters that you can adjust include port speed and duplex mode.

This chapter contains the following procedures:

- ❑ "Configuring Port Parameters" on page 74
- ❑ "Displaying Port Status" on page 81
- ❑ "Displaying Port Statistics" on page 85
- ❑ "Resetting a Port to the Default Settings" on page 88

Note

For further information about port parameters, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Configuring Port Parameters

To configure the parameter settings of a port on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Settings** tab.

The Port Settings tab is shown in Figure 18.

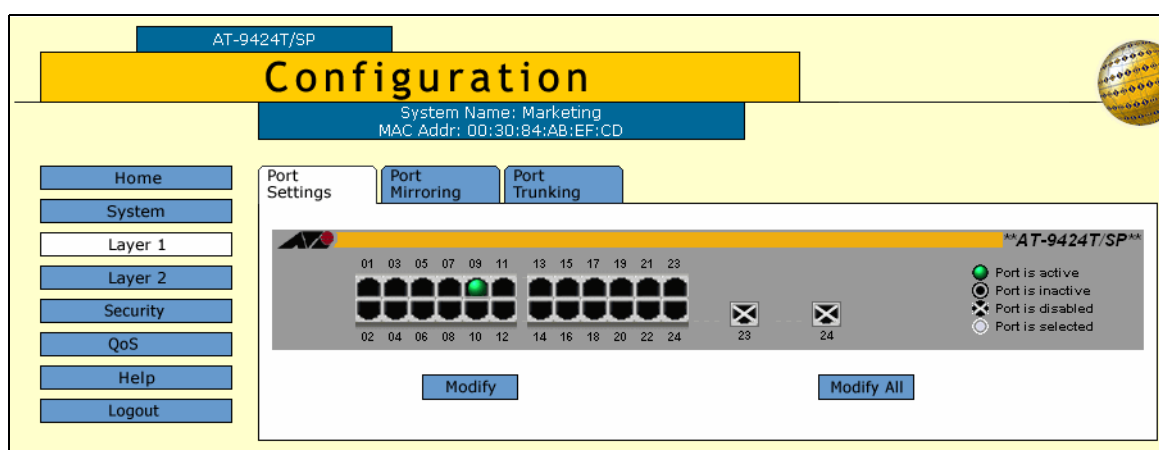


Figure 18. Port Settings Tab (Configuration)

4. Click the port in the graphical switch image that you want to configure. The selected port turns white. You can select more than one port at a time to configure. (To deselect a port, click it again.)
5. Click **Modify**. To configure all the ports, click **Modify All**.

Note

If you select **Modify All**, you cannot configure the port name or set the speed and duplex mode. The speed and duplex mode are set to autonegotiate.

The Port Configuration page is shown Figure 19.

The screenshot shows a web browser interface for 'Port Configuration - 5'. The page is divided into two main columns of settings. The left column includes fields for 'Port Name' (set to 'Port_05'), 'Speed and Duplex' (set to 'Auto-Negotiate'), 'Unknown Unicast Filter' (radio buttons for Disabled and Enabled), 'Flow Control' (radio buttons for Auto, Disabled, and Enabled), 'Flow Control/BackPressure Limit' (a text box with '000561' and a range '[1-7935] Cells'), 'Unknown Unicast Rate Limit' (radio buttons for Disabled and Enabled, with '262143' and range '[0-262143] Pkts/Sec'), and 'HOL Blocking' (radio buttons for Disabled and Enabled, with '008191' and range '[1-8191] Cells'). The right column includes 'Status' (radio buttons for Disabled and Enabled), 'Broadcast Filter' (radio buttons for Disabled and Enabled), 'Unknown Multicast Filter' (radio buttons for Disabled and Enabled), 'Back Pressure' (radio buttons for Disabled and Enabled), 'Broadcast Rate Limit' (radio buttons for Disabled and Enabled, with '262143' and range '[0-262143] Pkts/Sec'), 'Multicast Rate Limit' (radio buttons for Disabled and Enabled, with '262143' and range '[0-262143] Pkts/Sec'), and 'MDI/MDIX Crossover' (radio buttons for Auto, MDI, and MDIX). At the bottom of the form are three buttons: 'Apply', 'Defaults', and 'Close'.

Figure 19. Port Configuration Page

- Adjust the following parameters as necessary.

Port Name

Use this selection to assign a name to a port. The name can be from one to fifteen alphanumeric characters. Spaces are allowed, but you should not use special characters, such as asterisks or exclamation points. (You cannot assign a name when you are configuring more than one port.)

Status

Use this selection to enable or disable a port. When disabled, a port does not accept or forward frames.

You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. After the problem has been fixed, you can enable the port again to resume normal operation.

You might also want to disable a port that is not being used to secure it from unauthorized connections.

The possible settings are:

Enabled - The port receives and forwards packets. This is the default setting.

Disabled - The port does not receive or forward packets.

Speed and Duplex

You use this selection to configure a port for autonegotiation or to manually set a port's speed and duplex mode.

If you select Auto-Negotiate for autonegotiation, which is the default setting, the switch sets both speed and duplex mode for the port automatically.

Note the following about the operation of autonegotiation on the switch port:

- ☐ In order for a switch port to successfully autonegotiate its duplex mode with an end node, the end node should also be using autonegotiation. Otherwise, a duplex mode mismatch can occur. A switch port using autonegotiation defaults to half-duplex if it detects that the end node is not using autonegotiation. This results in a mismatch if the end node is operating at a fixed duplex mode of full-duplex.

To avoid this problem, when connecting an end node with a fixed duplex mode of full-duplex to a switch port, you should disable autonegotiation on the port and set the port's speed and duplex mode manually.

- ☐ If you disable autonegotiation on a port, the auto-MDI/MDI-X feature on a port is also disabled, and the port defaults to the MDI-X configuration. Consequently, if you disable autonegotiation and set a port's speed and duplex mode manually, you might also need to set the port's MDI/MDI-X setting as well.

Auto-Negotiate: The port autonegotiates both speed (10/100/1000 Mbps) and duplex mode. This is the default.

The other possible settings are:

10Mbps - Half Duplex

10Mbps - Full Duplex

100Mbps - Half Duplex

100Mbps - Full Duplex

Note

When a transceiver is inserted into an uplink slot and a link is established, that slot becomes a primary uplink port and the corresponding backup port, 23R or 24R, automatically transitions to redundant uplink status. The speed and duplex mode of the

redundant port automatically transitions to Auto-Negotiate to match the speed of the primary uplink port and you cannot configure the MDI/MDIX crossover parameter.

Note

1000 Mbps speed is only available when you set the port to autonegotiate. You cannot set this manually.

If you select all ports, the Speed and Duplex setting displays "Not Configurable," because all ports are set to autonegotiate.

Broadcast Filter

Use this parameter to limit the number of ingress broadcast packets the port receives. The possible settings are:

Enabled - The port does not receive any broadcast packets.

Disabled - The port receives broadcast packets. This is the default setting.

For further information about filters, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Unknown Unicast Filter

Use this parameter to limit the number of ingress unknown unicast packets the port receives. The possible settings are:

Enabled - The port does not receive any unknown unicast packets.

Disabled - The port receives unknown unicast packets. This is the default setting.

Unknown Multicast Filter

Use this parameter to limit the number of ingress unknown multicast packets the port receives. The possible settings are:

Enabled - The port does not receive any unknown multicast packets.

Disabled - The port receives unknown multicast packets. This is the default setting.

Flow Control

Sets flow control on a port. This option only applies to ports operating in full-duplex mode. A switch port uses back pressure to control the flow of ingress packets. The switch sends a special pause packet to stop the end node from sending frames. The

pause packet notifies the end node to stop transmitting for a specified period of time. The possible settings are:

Auto - The port uses flow control if it detects that the end node is using it.

Disabled - No flow control on the port. This is the default.

Enabled - Flow control is activated.

For further information about flow control, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Back Pressure

Use this parameter to set back pressure on a port. This option only appears for ports operating in half-duplex mode. A switch port uses back pressure to control the flow of ingress packets. The possible settings are:

Enabled - Back pressure is enabled.

Disabled - Back pressure is disabled. This is the default.

For further information about back pressure, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Flow Control/Back Pressure Limit

Use this parameter to specify the maximum number of ingress packets that a port receives within a one second period before initiating flow control or back pressure. The range is 1 to 7935 cells. The default is 561.

The following three parameters allow you to set rate limiting, the maximum number of ingress packets a port accepts each second. Packets exceeding the threshold are discarded.

Broadcast Rate Limit

Use this parameter to enable or disable ingress broadcast packet limits and specify a rate limit for the ingress broadcast packets. The possible settings are:

Enabled - Broadcast packet ingress rate limiting is enabled.

Disabled - Broadcast packet ingress rate limiting is disabled. This is the default.

You can also set the rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Unknown Unicast Rate Limit

Use this parameter to enable or disable ingress unknown unicast packet limits and specify a rate limit for the ingress unknown unicast packets. The possible settings are:

Enabled - Unknown unicast packet ingress rate limiting is enabled.

Disabled - Unknown unicast packet ingress rate limiting is disabled. This is the default.

You can also set the rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Multicast Rate Limit

Use this parameter to enable or disable ingress multicast packet limits and specify a rate limit for the ingress multicast packets. The possible settings are:

Enabled - Multicast packet ingress rate limiting is enabled.

Disabled - Multicast packet ingress rate limiting is disabled. This is the default.

You can also set the rate limit in packets per second. The range is 0 to 262143. The default is 262143.

HOL Blocking

HOL blocking sets a threshold on the utilization of a port's egress queue. When the threshold for a port is exceeded, the switch signals other ports to discard packets to the oversubscribed port. The possible settings are:

Enabled - HOL blocking prevention is activated.

Disabled - HOL blocking is inactivated on this port.

You also set the rate limit in number of cells. The range is 1 to 8191. The default is 8191. For more information about HOL blocking, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

MDI/MDIX Crossover

The wiring configuration of the port. The possible settings are:

Auto - The port automatically configures itself as MDI or MDIX, depending upon the end node. This is the default.

MDI - The port uses straight through cable.

MDIX - The port uses a crossover cable.

Note

Ports 23 and 24 are always set to Auto, and you cannot change the setting.

Note

The Auto setting is not available if you set a port's speed and duplex mode manually.

7. After you have made the desired changes, click **Apply**.

The switch activates the parameter changes on the port.

8. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying Port Status

To display the status of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 20.

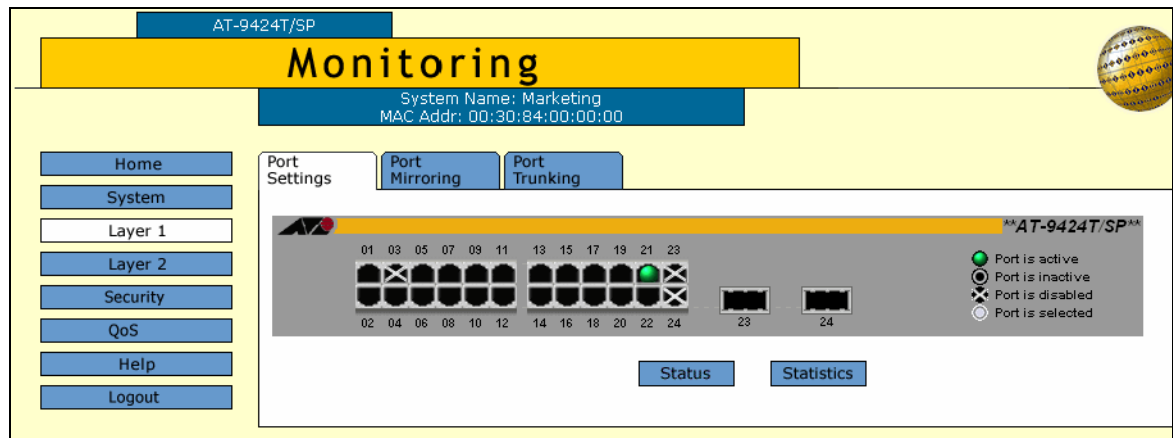


Figure 20. Port Settings Tab (Monitoring)

The Port Settings tab displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

3. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)
4. Click **Status**.

The Port Status page is shown in Figure 21.

Port Status - 3												
Total Ports Selected: 1. Page 1 of 1												
Port	Name	Link	Neg	MDI/X	Speed	Duplex	PVID	Flow Ctl	STP State	Filtering B-Bcast UM-Unknown Multicast UU-Unknown Unicast	HOL Blocking	Rate Limiting B-Bcast M-Multicast UU-Unknown Unicast
3	Port_03	Up	Auto	MDIX	0100	Full	1	Disabled	Disabled	B:Disabled UM:Disabled UU:Disabled	Enabled 8191 Cells	B:Disabled 262143 Pkts/Sec M:Disabled 262143 Pkts/Sec UU:Disabled 262143 Pkts/Sec -----
<input type="button" value="Refresh"/> <input type="button" value="Statistics"/> <input type="button" value="Close"/>												

Figure 21. Port Status Page

The Port Status page displays a table that contains the following columns of information:

Port

The port number.

Name

The name of the port.

Link

The status of the link between the port and the end node connected to the port. The possible settings are:

Up - A valid link exists between the port and the end node.

Down - The port and the end node have not established a valid link.

Neg

The status of autonegotiation on the port. The possible settings are:

Auto - Indicates that the port is using autonegotiation to set operating speed and duplex mode.

Manua - Indicates that the operating speed and duplex mode have been set manually.

MDI/X

The operating configuration of the port. The possible settings are MDI and MDI-X.

Speed

The operating speed of the port. The possible settings are:

0010 - 10 Mbps

0100 - 100 Mbps

1000 - 1000 Mbps

Duplex

The duplex mode of the port. The possible settings are half-duplex and full-duplex.

PVID

The VLAN

identifier (VID) of the VLAN in which the port is an untagged member. This column does not include the VIDs of the VLANs where the port is a tagged member.

Flow Control

The port's flow control setting. The possible settings are:

Enabled - Flow control is enabled on the port.

Disabled - Flow control is disabled on the port.

STP State

The operating status of the port. The possible settings are Forwarding and Disabled.

Filtering

Enables or disables filtering which discards ingress packets of a particular type. The possible settings are:

B-Bcast (Broadcast packet filtering) - The possible settings are enabled or disabled.

UM-Unknown Multicast (Unknown multicast packet filtering) - The possible settings are enabled or disabled.

UU-Unknown Unicast (Unknown unicast packet filtering) - The possible settings are enabled or disabled.

HOL Blocking

HOL blocking state. The possible settings are:

Enabled or disabled

of cells - Threshold number of cells.

Rate Limiting

The limit on the number of ingress packets of a particular type that the port accepts per second. The possible settings are:

B-Broadcast - Status of broadcast packet rate limit (enabled or disabled) and number of packets per second.

UM-Unknown Multicast - Status of unknown multicast packet filtering (enabled or disabled) and number of packets per second.

UU-Unknown Unicast - Status of unknown unicast packet filtering (enabled or disabled) and number of packets per second.

Displaying Port Statistics

To display the statistics of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 20 on page 81.

The Port Setting tab displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

3. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)
4. Click **Statistics**.

The Port Statistics page is shown in Figure 22.

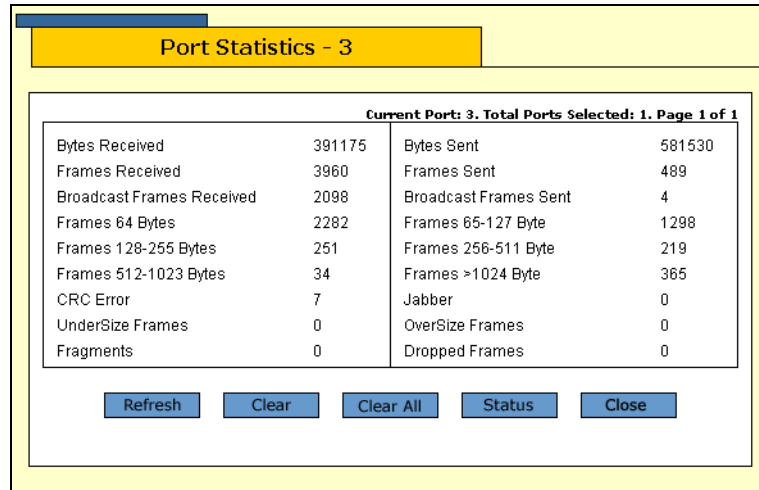


Figure 22. Port Statistics Page

The Port Statistics page displays a table that contains the following columns of information:

Bytes Received

Number of bytes received on the port.

Bytes Sent

Number of bytes transmitted from the port.

Frames Received

Number of frames received on the port.

Frames Sent

Number of frames transmitted from the port.

Broadcast Frames Received

Number of broadcast frames received on the port.

Broadcast Frames Sent

Number of broadcast frames transmitted from the port.

Multicast Frames Received

Number of multicast frames received on the port.

Multicast Frames Sent

Number of multicast frames transmitted from the port.

Frames 64 Bytes**Frames 65 - 127 Bytes****Frames 128 - 255 Bytes****Frames 256 - 511 Bytes****Frames 512 - 1023 Bytes****Frames > 1024 Bytes**

Number of frames transmitted from the port, grouped by size.

CRC Error

Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Jabber

Number of occurrences of corrupted data or useless signals appearing on the port.

No. of Rx Errors

Total number of frames received on the port containing errors.

Undersize Frames

Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Frames

Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragments

Number of undersized frames, frames with alignment errors, and

frames with frame check sequence (FCS) errors (CRC errors) received on the port.

Dropped Frames

Number of frames successfully received and buffered by the port, but discarded and not forwarded.

5. To clear all the counters for the selected port, click **Clear**. To clear the counters for all ports on the switch, click **Clear All**.

Resetting a Port to the Default Settings

To reset a port to the default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

3. Select the **Port Settings** tab.

The Port Settings tab is shown in Figure 18 on page 74.

4. Click the port in the graphical switch image that you want to configure. The selected port turns white. You can select more than one port at a time to configure. (To deselect a port, click it again.)

5. Click **Modify**. To configure all of the ports, click **Modify All**.

The Port Configuration page is shown Figure 19 on page 75.

6. Click **Defaults**.

The port(s) are returned to the default settings listed in Appendix A, "AT-S63 Default Settings" on page 357.

Chapter 7

MAC Address Table

This chapter contains instructions on how to add and view the dynamic and static addresses in the MAC address table of the switch. This chapter contains the following procedure:

- ❑ "Adding Static Unicast and Multicast MAC Addresses" on page 90
- ❑ "Deleting Unicast and Multicast MAC Addresses" on page 92
- ❑ "Deleting All Dynamic MAC Addresses" on page 93
- ❑ "Displaying the MAC Address Tables" on page 94
- ❑ "Changing the Aging Time" on page 97

Note

For background information on MAC address tables, refer to Chapter 7, "MAC Address Table," in the *AT-S63 Management Software Menus Interface User's Guide*.

Adding Static Unicast and Multicast MAC Addresses

This section contains the procedure for assigning a static unicast or multicast address to a port on the switch. You can assign up to 255 static MAC addresses per port.

To add a static address to the MAC address table, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 23.

The screenshot displays the Configuration page for a switch, specifically the Layer 2 tab. The top navigation bar includes 'Home', 'System', 'Layer 1', 'Layer 2' (selected), 'Security', 'QoS', 'Help', and 'Logout'. The main content area is titled 'Configuration' and shows system information: 'System Name: Marketing' and 'MAC Addr: 00:30:84:AB:EF:CD'. Below this, there are tabs for 'MAC Address' (selected), 'VLAN', 'GVRP', 'Spanning Tree', and 'Enhanced Stacking'. The 'MAC Address' section is divided into three main areas:

- View/Add Unicast MAC Addresses:** This section contains radio buttons for 'View All' (selected), 'View Static', and 'View Dynamic'. To the right, there are options to 'View MAC Addresses on Port(s)' and 'View MAC Addresses for VLAN', each with a corresponding input field. Below these is a MAC address input field in the format 'XX:XX:XX:XX:XX:XX'.
- View/Add Multicast MAC Addresses:** This section contains radio buttons for 'View All', 'View Static', and 'View Dynamic'. To the right, there are options to 'View MAC Addresses on Port(s)' and 'View MAC Addresses for VLAN', each with a corresponding input field. Below these is a MAC address input field in the format 'XX:XX:XX:XX:XX:XX'.
- Delete All Dynamic MAC Addresses:** This section contains a text box with the instruction 'Click "Delete" to Remove All Dynamic MAC Addresses.' and a 'Delete' button.

Figure 23. MAC Address Tab (Configuration)

3. To add a static unicast address, in the View/Add Unicast MAC Addresses section, click **Add**. To add a static multicast address, in the View/Add Multicast MAC Addresses section, click **Add**.

The Add MAC Address page is shown in Figure 24.

Figure 24. Add MAC Address Page

4. Adjust the following parameters as necessary.

MAC Address

The new static unicast or multicast MAC address.

Port Number

The number of the port on the switch where you want to assign the static address. If you are adding a static unicast address, you can enter only one port.

If you are entering a static multicast address, you must specify the port when the multicast application is located as well as the ports where the host nodes are connected. Assigning the address only to the port where the multicast application is located results in the failure of the multicast packets to be properly forwarded to the host nodes. You can specify the ports individually (e.g., 1,4,5), as a range (e.g., 11-14) or both (e.g., 15-17,22,24).

VLAN ID

The VLAN ID where the port is a member.

5. Click **Apply**.
6. Repeat this procedure to add other static addresses to the switch.
7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Deleting Unicast and Multicast MAC Addresses

To delete a static or dynamic unicast or multicast MAC address from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Display the MAC addresses on the switch by selecting one of the options.

For detailed instructions, refer to "Displaying the MAC Address Tables" on page 94.

4. Click the button next to the MAC address that you want to delete from the switch.

5. Click **Remove**.

Note

You cannot delete a switch's MAC address, an STP BPDU MAC address, or a broadcast address.

6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Deleting All Dynamic MAC Addresses

To delete all the dynamic MAC addresses, unicast or multicast, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. In the Delete All Dynamic MAC Addresses section, click **Delete**.

Displaying the MAC Address Tables

To view the MAC address table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25.

The screenshot shows a web interface for a network device. At the top, there's a header bar with 'AT-9424T/SP' and a large yellow 'Monitoring' button. Below this, a blue bar displays 'System Name: Marketing' and 'MAC Addr: 00:30:84:00:00:00'. A left sidebar contains navigation buttons: Home, System, Layer 1, Layer 2 (highlighted), Security, QoS, Help, and Logout. The main content area has tabs for 'MAC Address' (selected), 'VLAN', 'Spanning Tree', 'Port Security', and 'Enhanced Stacking'. Under the 'MAC Address' tab, there are two sections: 'View Unicast MAC Addresses' and 'View Multicast MAC Addresses'. Each section has three radio button options: 'View All', 'View Static', and 'View Dynamic'. To the right of these options are two more radio button options: 'View MAC Addresses on Port(s)' with a text input field, and 'View MAC Addresses for VLAN' with a text input field. Below these is a MAC address input field in the format ' : : : : : '. Each section has a 'View' button at the bottom.

Figure 25. MAC Address Tab (Monitoring)

The tab contains two sections. The upper section displays unicast addresses; the lower part displays multicast addresses. The options function the same in both sections, and are described below. You can select only one option at a time.

View All

Displays all dynamic addresses learned on the ports of the switch and all static addresses that have been assigned to the ports.

View Static

Displays just the static addresses assigned to the ports on the switch.

View Dynamic

Displays only the dynamic addresses learned on the ports on the switch.

View MAC Addresses on Port

Displays the dynamic and static MAC addresses of a particular port. You can specify more than one port at a time.

View MAC Addresses for VLAN

Displays the static and dynamic addresses learned on the tagged and untagged ports of a specific VLAN. You specify the VLAN by entering the VLAN ID number. You can specify only one VLAN at a time.

View MAC Address

Displays the port number on which a MAC address was assigned or learned.

In some situations, you might want to know on which port a particular MAC address was learned. You could display the MAC address table and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding the address could prove difficult.

The View MAC Address option allows you to specify the MAC address and let the AT-S63 management software automatically locate the port on the switch where the device is connected.

3. After you select an option, click **View**.

Figure 26 shows an example of viewing all unicast MAC addresses.

View MAC Addresses

Total MAC Addresses: 117. Page 1 of 12

VLAN ID	MAC ADDRESS	PORT(s)	TYPE
1	00:00:CD:01:6B:5D	5	Dynamic
1	00:00:CD:0D:40:CC	5	Dynamic
1	00:00:F4:A4:12:44	5	Dynamic
1	00:00:F4:DD:29:31	5	Dynamic
1	00:02:2D:7B:AA:EA	5	Dynamic
1	00:02:2D:7C:AF:F9	5	Dynamic
1	00:02:55:B1:1E:98	5	Dynamic
1	00:02:DD:32:3D:1C	5	Dynamic
1	00:04:23:56:70:6B	5	Dynamic
1	00:04:23:80:B3:0E	5	Dynamic

Refresh

Next

Close

Figure 26. View MAC Addresses Page

The View MAC Addresses page displays a table that contains the following columns of information:

VLAN ID

The ID number of the VLAN where the port is a member.

MAC Address

The static or dynamic unicast MAC address.

Port(s)

The port on which the address was learned or assigned. The MAC address with port "CPU" is the address of the switch.

Type

The type of the address: static or dynamic.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default setting for the aging time is 300 seconds (5 minutes).

To adjust the aging time, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. In the Configuration section, for the MAC Address Aging Time item, enter a new value in seconds. The range is 8 to 512 seconds. The default is 300 seconds (5 minutes).
3. Click **Apply**.
4. To permanently save the change, click **Save Changes**.

Chapter 8

Port Trunking

This chapter contains the procedure for creating, modifying, or deleting a port trunk. The sections in this chapter are:

- ❑ "Creating a Port Trunk" on page 100
- ❑ "Modifying a Port Trunk" on page 103
- ❑ "Deleting a Port Trunk" on page 105
- ❑ "Displaying the Port Trunks" on page 106

Note

For background information on port trunking, refer to Chapter 8, "Port Trunking," in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Port Trunk



Caution

Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms, which can adversely effect the operation of your network.

If you are deleting a port trunk, disconnect the cables from the ports before you delete the trunk. Deleting the trunk without first disconnecting the data cables can create a loop in your network topology, which can result in broadcast storms.

To create a port trunk, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 27.

ID	Name	Type	Ports
1	Server11	SA/DA	12-16

Figure 27. Port Trunking Tab (Configuration)

Any existing trunks are shown in a table.

4. Click **Add**.

The Add New Trunk page is shown in Figure 28.

Figure 28. Add New Trunk Page

5. Adjust the following parameters as necessary.

Trunk Name

The name for the port trunk. The name can be up to 16 alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must be given a unique name.

Trunk Method

Select a load distribution method. The possible settings are:

SA - Source MAC address (Layer 2)

DA - Destination MAC address (Layer 2)

SA/DA - Source MAC address /destination MAC address (Layer 2)

SI - Source IP address (Layer 3)

DI - Destination IP address (Layer 3)

SI/DI - Source IP address /destination IP address (Layer 3)

6. Click the ports that are to make up the port trunk. A selected port changes to white. An unselected port is black. A port trunk can contain up to eight ports.

Note

All ports in a trunk must operate at the same speed. When you include port 23R or 24R in a trunk and the port transitions to redundant uplink status, the port speed is automatically adjusted to

1000 Mbps. If the other ports in the trunk are operating at a different speed, port trunking may be unpredictable. Because of these port speed variables, Allied Telesyn suggests that you not include port 23R or 24R in a port trunk.

7. Click **Apply**.

The new port trunk is now active on the switch.

8. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

9. Configure the ports on the remote switch for port trunking.
10. Connect the cables to the ports of the trunk on the switch.

The port trunk is ready for network operations.

Modifying a Port Trunk

This section contains the procedure for modifying a port trunk on the switch. You can change the name of a trunk and the ports that constitute the trunk. You cannot change the load distribute method. Be sure to review the guidelines in Chapter 8, "Port Trunking," in the *AT-S63 Management Software Menus Interface User's Guide* before you perform the procedure:



Caution

If you are adding or removing ports from the trunk, you should disconnect all data cables from the ports of the trunk on the switch before performing the procedure: Adding or removing ports from a port trunk without first disconnecting the cables may result in loops in your network topology. Loops can produce broadcast storms and poor network performance.

Note

Before you modify a port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port that are to be in the trunk. Check to be sure that the settings are correct for the end node to which the trunk is to be connected. When you modify a trunk, the AT-S63 management software copies the settings of the lowest numbered port in the trunk to the other ports so that all the settings are the same.

You should also check to be sure that the ports are untagged members of the same VLAN. You cannot create a trunk of ports that are untagged members of different VLANs.

To modify a port trunk, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 27 on page 100.

4. Click the button next to the port trunk you want to modify and click **Modify**.

The Modify Trunk page is shown in Figure 29.

Figure 29. Modify Trunk Page

Note

You cannot change the Trunk ID number or the load distribution method of a port trunk.

- Adjust the following parameter as necessary.

Trunk Name

The name can be up to 16 alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must have a unique name.

- To add or remove ports from a trunk, click the ports in the graphical image of the switch. A selected port changes to white. An unselected port is black. A port trunk can contain up to eight ports.
- Click **Apply**.

Changes to a port trunk are activated on the switch.

- To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

- Reconnect the cables to the ports of the trunk.

Deleting a Port Trunk



Caution

Disconnect the cables from the port trunk on the switch before performing the following procedure: Deleting a port trunk without first disconnecting the cables can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

To delete a port trunk from the switch, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 27 on page 100.

4. Click the button next to the port trunk you want to delete and click **Remove**.

The port trunk is deleted from the switch.

5. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying the Port Trunks

To display the port trunks, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44

2. From the Monitoring menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 20 on page 81.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 30.

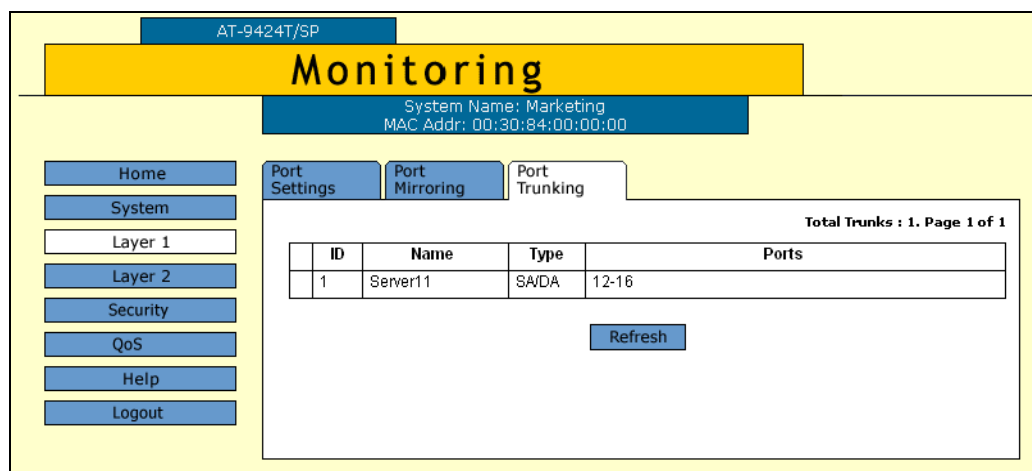


Figure 30. Port Trunking Tab (Monitoring)

The Port Trunking tab displays a table that contains the following columns of information:

ID

The ID number of the trunk.

Name

The name of the trunk.

Type

The load distribution method. The possible settings are:

SA - Source MAC address (Layer 2)

DA - Destination MAC address (Layer 2)

SA/DA - Source MAC address /destination MAC address (Layer 2)

SI - Source IP address (Layer 3)

DI - Destination IP address (Layer 3)

SI/DI - Source IP address /destination IP address (Layer 3)

Ports

The ports of the trunk.

Chapter 9

Port Mirroring

This chapter contains the procedure for creating or deleting a port mirror. The sections in the chapter include:

- ❑ "Creating a Port Mirror" on page 110
- ❑ "Modifying a Port Mirror" on page 113
- ❑ "Disabling a Port Mirror" on page 114
- ❑ "Deleting a Port Mirror" on page 115
- ❑ "Displaying the Port Mirror" on page 116

Note

For background information on port mirroring, refer to Chapter 9, "Port Mirroring," in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Port Mirror

To create a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 31.

Mirror to Port	Ingress Port(s)	Egress Port(s)	Status
11	1,7-9	2,7-9	Enabled

Figure 31. Port Mirroring Tab (Configuration)

This tab displays any port mirror already existing on the switch. If the Mirror to Port column contains a 0 (zero), there is no port mirror.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 32.

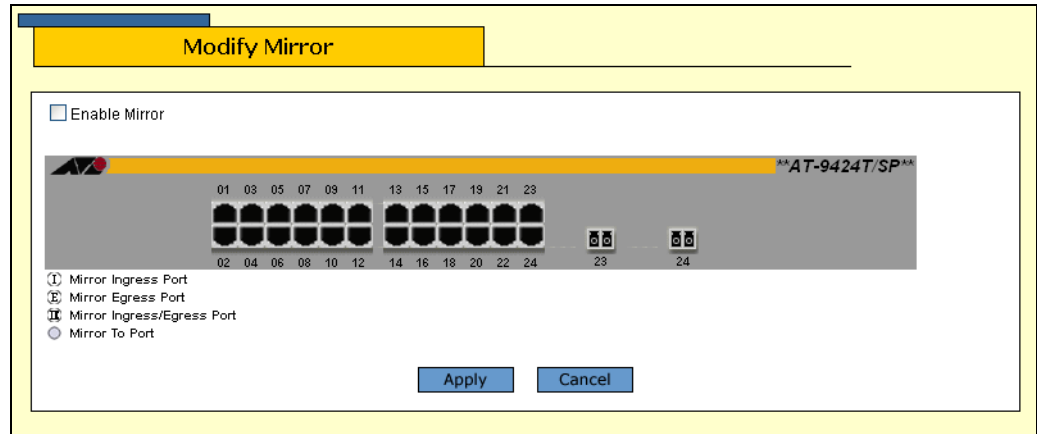


Figure 32. Modify Mirror Page

- Click the ports of the port mirror. Clicking a port toggles it through the possible settings, which are as follows:



The destination (mirror) port. There can be only one destination port.



A source port. The port's ingress traffic is mirrored to the destination port.



A source port. The port's egress traffic is mirrored to the destination port.



A source port. The port's ingress and egress traffic is mirrored to the destination port.

You can mirror just one port, a few ports, or all of the ports on the switch, with the exception, of course, of the destination port.

Note

When a transceiver is inserted into an uplink slot and a link is established, that slot becomes a primary uplink port and the corresponding backup port, 23R or 24R, automatically transitions to redundant uplink status. Any settings for port mirroring remain intact when the backup port makes the transition to a redundant uplink state.

Figure 33 shows an example of the Modify Mirror page configured for a port mirror. The egress traffic on ports 11 and 12 is being mirrored to the destination port 5.

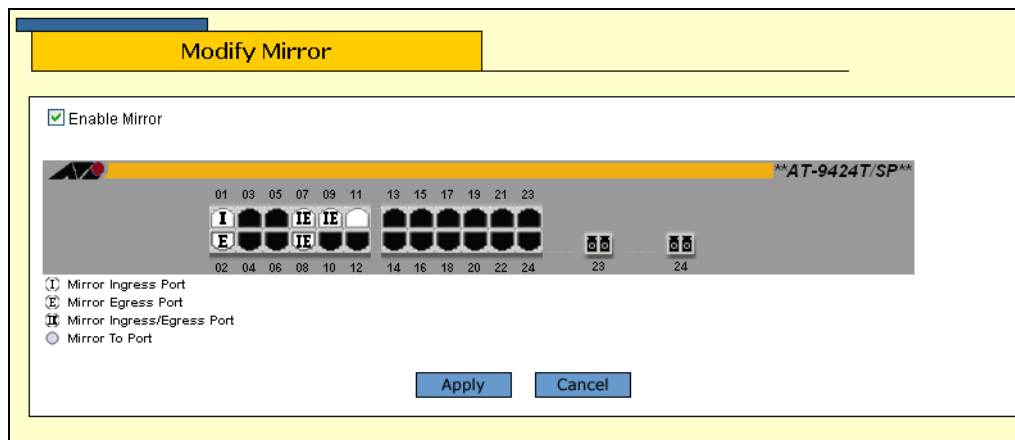


Figure 33. Example of a Modify Mirror Page

6. After selecting the destination and source ports, click the **Enable Mirror** check box.
7. Click **Apply**.

The port mirror is now active on the switch. You can connect a data analyzer to the destination port to monitor the traffic on the source ports.

8. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Modifying a Port Mirror

To modify a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 31 on page 110.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 32 on page 111.

5. Click the ports of the port mirror to change its type. Clicking a port toggles it through the possible settings, which are as follows:



The destination (mirror) port. There can be only one destination port.



A source port. The port's ingress traffic is mirrored to the destination port.



A source port. The port's egress traffic is mirrored to the destination port.



A source port. The port's ingress and egress traffic is mirrored to the destination port.

6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Disabling a Port Mirror

To disable a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 31 on page 110.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 32 on page 111.

5. Click the **Enable Mirror** checkbox to remove the check and disable the mirror.

6. Click **Apply**.

7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Deleting a Port Mirror

To delete a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 31 on page 110.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 32 on page 111.

5. Click the **Enable Mirror** checkbox to remove the check and disable the mirror.

6. Click **Apply**.

7. Click the destination port, which is white, so that it is black.

8. Click **Apply**.

9. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying the Port Mirror

To display the port mirror, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44

2. From the Monitoring menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 20 on page 81.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 34.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

Port Settings Port Mirroring Port Trunking

Total Mirrors: 1. Page 1 of 1

Mirror to Port	Ingress Port(s)	Egress Port(s)	Status
11	1,7-9	2,7-9	Enabled

Refresh

Figure 34. Port Mirroring Tab (Monitoring)

The Port Mirroring tab displays a table that contains the following columns of information:

Mirror to Port

The destination port to which the traffic is copied and where the network analyzer is located.

Ingress Port(s)

The source ports whose ingress traffic is mirrored to the destination port.

Egress Port(s)

The source ports whose egress traffic is mirrored to the destination port.

Status

The status of the mirroring feature. The possible settings are:

Enabled - Traffic is being copied to the destination port.

Disabled - No traffic is being mirrored.

Section II

Advanced Features

The chapters in this section explain additional switch management features of the AT-S63 management software. The chapters include:

- ❑ Chapter 10, "File Downloads and Uploads" on page 121
- ❑ Chapter 11, "Event Log" on page 127
- ❑ Chapter 12, "Quality of Service" on page 141
- ❑ Chapter 13, "IGMP Snooping" on page 153
- ❑ Chapter 14, "STP and RSTP" on page 163
- ❑ Chapter 15, "MSTP" on page 181

Chapter 10

File Downloads and Uploads

This chapter contains the procedure for downloading a new AT-S63 image file onto the switch. This chapter also contains procedures for uploading and downloading system files, such as a boot configuration file, from the file system in the switch. This chapter contains the following sections:

- ❑ "Downloading a File" on page 122
- ❑ "Uploading a File" on page 125

Downloading a File

This procedure explains how to download a file from a TFTP server on your network to the switch using the web browser interface. You can download any of the following files:

- ☐ AT-S63 image file
- ☐ Boot configuration file
- ☐ Public key
- ☐ CA certificate

Note

The public key and CA certificate are supported only on the version of AT-S63 management software that features SSL, PKI, and SSH security.

Note the following before you begin this procedure:

- ☐ You must use TFTP to download a file from a web browser management session.
- ☐ To use TFTP, there must be a node on your network that contains the TFTP server software.
- ☐ The file that you are downloading must be stored on the TFTP server node.
- ☐ You should start the TFTP server before you begin the download procedure:
- ☐ The AT-S63 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- ☐ Installing a new AT-S63 software image does not change the current configuration of a switch (for instance, IP address, subnet mask, and virtual LANs). If you want to return a switch to its default configuration values, refer to "Returning the AT-S63 Management Software to the Factory Default Values" on page 50.



Caution

The switch stops forwarding Ethernet traffic after it has downloaded an AT-S63 image file and begun to initialize the software. Some network traffic may be lost.

To download a file, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default.

2. Select the **System Utilities** tab.

The System Utilities tab is shown in Figure 35.

The screenshot shows the AT-S63 Management Software Web Browser Interface. At the top, there is a blue header bar with the text "AT-9424T/SP". Below this is a yellow banner with the word "Configuration" in large black font. Under the banner, there is a blue box containing the text "System Name: Marketing" and "MAC Addr: 00:30:84:AB:EF:CD". To the left of the main content area is a vertical sidebar with buttons: "Home", "System", "Layer 1", "Layer 2", "Security", "QoS", "Help", and "Logout". The main content area has a top row of tabs: "General", "SNMP", "IGMP", "System Utilities", "Server-based Authentication", and "Event Log". The "System Utilities" tab is selected. Below the tabs, there is a checkbox labeled "Reboot Switch After Resetting to Defaults" with an "Apply" button to its right. Below this is a section titled "TFTP File Uploads and Downloads". This section contains two columns of fields. The left column has "TFTP Server IP Address" (a dotted box with four zeros), "TFTP Remote Filename" (a text input field), and "TFTP FileType" (radio buttons for "Image", "Default Config", and "General", with "Image" selected). The right column has "TFTP Operation" (radio buttons for "Download" and "Upload", with "Download" selected) and "TFTP Local Filename" (a text input field). An "Apply" button is located at the bottom right of the TFTP section.

Figure 35. System Utilities Tab (Configuration)

Note

You use the top portion of the tab to return the switch to its factory default settings. For instructions, refer to "Returning the AT-S63 Management Software to the Factory Default Values" on page 50.

3. In the TFTP Server IP Address field, enter the IP address of the network node that contains the TFTP server software.
4. In the TFTP Operation field, click **Download**.
5. In the TFTP Remote Filename field, enter the filename of the file on the TFTP server to be downloaded to the switch.
6. In the TFTP Local Filename field, enter a name for the file. This is the name that the switch uses to store the file in its file system. If you are downloading the AT-S63 image file, enter "ats62.img" as the filename.
7. For the TFTP File Type, select one of the following:

Image

Select this option if you are downloading the AT-S63 image file.

Default Config

Select this option if you are downloading a configuration file and you want the file to be designated as the active boot configuration file.

General

Select this option if you are downloading a CA certificate or encryption key, or a configuration file that you do not want designated as the active boot configuration file.

8. Click **Apply.**

The management software notifies you after the download is complete.



Caution

After an AT-S63 switch image file is downloaded, the switch must decompress it and write it to flash. This can require one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file. After the file has been decompressed, the switch automatically resets. Your web browser management session ends. To continue managing the switch, you must reestablish the management session.

Uploading a File

This procedure explains how to upload a file from the switch's file system to a TFTP server on your network using the web browser interface. You can upload any of the following files:

- ☐ Boot configuration file
- ☐ Public encryption key
- ☐ CA certificate
- ☐ CA enrollment request

Note

The public key, CA certificate, and CA enrollment request are supported only on the version of AT-S63 management software that features SSL, PKI, and SSH security.

Note the following before you begin this procedure:

- ☐ You must use TFTP to download a file from a web browser management session.
- ☐ There must be a node on your network that contains the TFTP server software.
- ☐ You should start the TFTP server before you begin the upload procedure:

To upload a file, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default.

2. Select the **System Utilities** tab.

The System Utilities tab is shown in Figure 35 on page 123.

Note

The top portion of the tab is used to return the switch to its factory default settings. For instructions, refer to "Returning the AT-S63 Management Software to the Factory Default Values" on page 50.

3. In the TFTP Server IP Address field, enter the IP address of the network node that contains the TFTP server software.

4. In the TFTP Operation field, click **Upload**.
5. In the TFTP Remote Filename field, enter a name for the file. This is the name that the file is stored as on the TFTP server.
6. In the TFTP Local Filename field, enter the name of the file in the switch's file system that you want to upload to the TFTP server.

Note

The TFTP File Type options are not used when uploading a file.

7. Click **Apply**.

The management software notifies you when the upload is complete.

Chapter 11

Event Log

This chapter describes the event log that allows you to view information about network activity. Sections in the chapter include:

- ❑ "Enabling or Disabling the Event Log" on page 128
- ❑ "Displaying Events" on page 130
- ❑ "Disabling the Event Log" on page 137
- ❑ "Clearing the Event Log" on page 138
- ❑ "Saving the Event Log to a File" on page 139

For more information about the event log, refer to the *AT-S63 Management Software Web Browser Interface User's Guide*.

Note

The event log, even when disabled, logs all AT-S63 initialization events that occur when the switch is reset or power cycled. Any switch events that occur after AT-S63 initialization are entered into the log only if you enable the event log. The default setting for the event log is disabled.

Enabling or Disabling the Event Log

To enable or disable the event log, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 36.

The screenshot shows the 'Configuration' page for a device (AT-9424T/SP). The 'Event Log' tab is selected. The page is divided into two main sections: 'Log Settings' and 'Filter Settings and Actions'.

Log Settings:

- Status:** Radio buttons for 'Disabled' and 'Enabled' (selected).
- Log Full Action:** Radio buttons for 'Wrap' (selected) and 'Halt'.
- Clear Log:** A checkbox for 'Clear Log' is present, with radio buttons for 'Permanent' and 'Temporary' (selected).

Filter Settings and Actions:

- Log Location:** Radio buttons for 'Temporary (RAM)' (selected) and 'Permanent(NVS)'.
- Severity Selections:** A list box showing 'D-Debug', 'E-Error', 'W-Warning', and 'Information'.
- Display Order:** Radio buttons for 'Chronological' (selected) and 'Reverse Chronological'.
- Mode:** Radio buttons for 'Normal' (selected) and 'Full'.
- Module Selections:** A list box showing 'SYSTEM', 'CLI', 'EVTLOG', and 'MAC'.
- Save Filename:** An empty text input field.

Buttons for 'Apply', 'View', and 'Save' are located at the bottom of the configuration area.

Figure 36. Event Log Tab (Configuration)

3. In the Log Settings section, for the Status, click **Enabled** to enable the event log, or **Disabled** to disable the event log.

The event log is enabled by default.

4. To determine what action the switch takes when the event log reaches its maximum capacity, for the **Log Full Action**, click one of the following:

Wrap

When the event log reaches its maximum capacity, this option deletes old entries and continues to add new entries. This is the default.

Halt

When the log file reaches its maximum capacity, the log stops adding new entries.

5. Click **Apply** to activate the settings on the switch.
6. Select the **General** tab.
7. Click **Save Changes** to permanently save your changes. (This button is not displayed if there are no changes to save.)

Displaying Events

Each time that you want to view the event log, you must choose how and what you want displayed. The event log settings are not saved.

To specify the type of events you want to display in the event log, perform the following procedure:

1. From the home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

Note

You can also display events by selecting Configuration from the home page and then the Event Log tab. The tab contains the same Filter Settings and Actions section as described in this procedure:

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 37.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

General SNMP IGMP Ping Client Server-based Authentication **Event Log**

Filter Settings and Actions

Log Location
☒ Temporary (RAM)
☐ Permanent (NVS)

Severity Selections
 D-Debug
 E-Error
 W-Warning
 I-Information

Display Order
☒ Chronological
☐ Reverse Chronological

Mode
☒ Normal
☐ Full

Module Selections
 SYSTEM
 CLI
 EVTLOG
 MAC

View

Figure 37. Event Log Tab (Monitoring)

3. In the Filter Settings and Actions section, for **Log Location**, click one of the following:

Temporary (Memory)

Displays the events stored in temporary memory. This selection stores approximately 4,000 events. If the switch has been running for some time without a reset or power cycle, select Temporary. This is the default.

Permanent (NVS)

Displays events stored in nonvolatile memory, which stores no more than 2,000 events. If the switch was recently reset or power cycled and you want to view the events that occurred prior to the reset, select Permanent.

4. To display events of a selected severity, in the **Severity Selections** list, select one or more of the following severity types:

D - Debug

Debug messages provide detailed high-volume information that is intended only for technical support personnel.

E - Error

Only error messages are displayed. Error messages indicate that the switch operation is severely impaired.

W - Warning

Only warning messages are displayed. These messages indicate that an issue may require manager attention.

I - Information

Only informational messages are displayed. Informational messages display useful information that you can ignore during normal operation.

ALL

All messages of any type are displayed.

To select more than one severity, use <Ctrl> click.

5. To choose the chronological order of events in the display, for **Display Order**, click one of the following:

Chronological

Displays the events in the order from the oldest event to the most recent event. This is the default.

Reverse Chronological

Displays the events in from the most recent event to the oldest event.

6. To select the format of the event log, for **Mode**, click one of the following:

Normal

Displays the time, module, severity, and description for each event. This is the default. An example of Normal mode is shown in Figure 38 on page 134.

Full

Displays the same information as Normal, plus the file name, line number, and event ID. An example of Full mode is shown in Figure 39 on page 135.

7. To display events of a particular AT-S63 software module, from the **Module Selections** list, select one or more of the modules listed in Table 1. To select more than one module, use <Ctrl> click.

Table 1. AT-S63 Software Modules

Name	Description
ACL	Access control lists
ALL	All modules
CFG	Configuration file
CLI	Command line interface commands
DOS	Denial of Service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP VLAN Registration Protocol
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	IP configuration
MAC	MAC address table
MGMTACL	Management ACL
PACCESS	802.1X Port-based Access Control
PCFG	Port configuration
PKI	Public Key Infrastructure

Table 1. AT-S63 Software Modules (Continued)

Name	Description
PMIRR	Port mirroring
PSEC	Port security
PTRUNK	Port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RRP	RRP Snooping
SNMP	Simple Network Management Protocol
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; Manager and Operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	TELNET
TFTP	Trivial File Transfer Protocol
TIME	System Time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes

8. Click **View**.

Figure 38 shows an example of an event log in Normal mode.

Events View - NormalMode		
Severity	Date and Time	Event
I	04/20/04 06:56:54	file: File System initialized
I	04/20/04 06:56:54	http: Server reset to defaults
I	04/20/04 06:56:54	ssh: SSH server disabled
I	04/20/04 06:56:55	cfg: Configuration initialized
I	04/20/04 06:56:55	tacacs: TACACS+ initialized
I	04/20/04 06:56:55	radius: RADIUS initialized
I	04/20/04 06:56:55	garp: GARP initialized
I	04/20/04 06:56:56	qos: Number of Egress Queues set to 8
I	04/20/04 06:56:56	qos: Priority 0 mapped to Egress Queue 0
I	04/20/04 06:56:56	qos: Priority 1 mapped to Egress Queue 1

Figure 38. Event Log Example Displayed in Normal Mode

The events are displayed in a table. The columns in the table shown in normal display mode are described below:

S (Severity)

The event's severity. The severity codes and their corresponding severity level and description are shown in Table 2.

Table 2. Event Severity Levels

Severity Code	Severity Level	Description
E	Error	Switch operation is severely impaired.
W	Warning	An issue that may require network manager attention.
I	Information	Useful information that can be ignored during normal operation.
D	Debug	Messages intended for technical support and software development.

Date and Time

The date and time the event occurred.

Event

This item contains two parts. The first part is the name of the module within the AT-S63 management software that generated the event. The second part is a description of the event.

When you display the events in full mode, more information is included. Figure 39 shows the same portion of the event log in Figure 38 on page 134 but displayed in full mode.

Events View - FullMode				
Severity	Date and Time	EventID	Filename:Line	Event
I	04/20/04 06:56:54	183001	fileapp.c:131	file: File System initialized
I	04/20/04 06:56:54	243004	webserv.c:79	http: Server reset to defaults
I	04/20/04 06:56:54	323003	atiss.h.c:535	ssh: SSH server disabled
I	04/20/04 06:56:55	363001	cfgmain.c:159	cfg: Configuration initialized
I	04/20/04 06:56:55	283001	tacacs.c:830	tacacs: TACACS+ initialized
I	04/20/04 06:56:55	273001	radiusclient.c:1280	radius: RADIUS initialized
I	04/20/04 06:56:55	073001	garpmain.c:259	garp: GARP initialized
I	04/20/04 06:56:56	203002	qosapp.c:711	qos: Number of Egress Queues set to 8
I	04/20/04 06:56:56	203003	qosapp.c:787	qos: Priority 0 mapped to Egress Queue 0
I	04/20/04 06:56:56	203003	qosapp.c:787	qos: Priority 1 mapped to Egress Queue 1

[Close](#)

Figure 39. Event Log Example Displayed in Full Mode

In addition to the information displayed in Normal mode, the Full mode also displays additional columns in the table, as described below:

Event ID

A unique, random number assigned to each event.

Filename:Line

The AT-S63 software source file name and the line number in that source file that produced the event.

- Click one of the following buttons to scroll through the event log:

Last - Last page

First - First page

Next - Next page

Previous - Previous page

Close - Closes the log

To clear the current event log, go to "Clearing the Event Log" on page 138.

Disabling the Event Log

To activate or deactivate the event log, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 36 on page 128.

3. In the Log Settings section, for the Status, click **Disabled**.

4. Click **Apply** to activate the settings on the switch.

5. Select the **General** tab.

6. Click **Save Changes** to permanently save your changes. (This button is not displayed if there are no changes to save.)

Clearing the Event Log

You can clear the event log to remove old events and start fresh. To clear the event log, do the following:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 36 on page 128.

3. In the Log Settings section, click the **Clear Log** checkbox.
4. Click the button next to the location of the log you want to clear, either Permanent or Temporary.
5. Click **Apply** to activate the settings on the switch.

Saving the Event Log to a File

You can save the event log to a file to review later. The file is saved as an ASCII file so that you can also email the file to someone else for troubleshooting.

To save the event log to a file, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 36 on page 128.

3. In the **Filter Settings and Actions** section, select the type of events you want to save to the file.

4. In the **Save Filename** field, enter a name for the file with a .log file name extension.

5. Click **Save**.

The log file is saved on the switch as an ASCII file.

6. To upload the file to your management station for viewing or sending with an email, refer to "Uploading a File" on page 125.

Chapter 12

Quality of Service

This chapter contains instructions on how to configure Quality of Service (QoS). This chapter contains the following procedure:

- ❑ "Configuring CoS" on page 142
- ❑ "Mapping CoS Priorities to Egress Queues" on page 145
- ❑ "Configuring Egress Scheduling" on page 148
- ❑ "Displaying the CoS Settings" on page 150
- ❑ "Displaying the QoS Schedule" on page 152

Note

For background information on QoS, refer to Chapter 13, "Quality of Service," in the *AT-S63 Management Software Menu Interface User's Guide*.

Configuring CoS

This procedure explains how to change the egress queue used to handle untagged ingress packets on a port. This procedure also overrides the priority levels in tagged ingress packets.

To configure CoS, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **QoS** option.

The QoS page is displayed with the CoS tab selected by default, as shown in Figure 40.

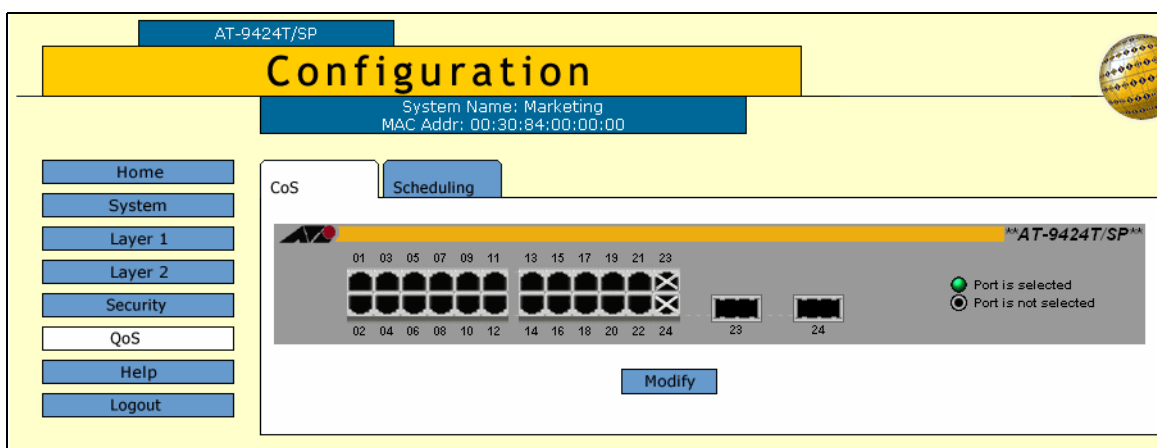


Figure 40. CoS Tab (Configuration)

3. Click the port where you want to configure CoS. You can select more than one port at a time. A selected port turns white. (To deselect a port, click it again.)
4. Click **Modify**.

The CoS Setting for Port page is shown in Figure 41.

Port	VLAN Id	Default Priority	Override Priority
2	1	0	No

Priority Level 0 ▼ ☐ Override Priority

Apply Cancel

Figure 41. CoS Setting for Port Page

- Use the Priority list to select a value from Level 1 to Level 7 that corresponds to the egress queue where you want all untagged ingress packets on the port to be stored. For example, if you select Level 4, all untagged packets received on the port are stored in egress queue Q2 of the egress port. The default is Level 0, which corresponds to Q0. (If you perform Step 6 and override the priority level in tagged packets, the selected egress queue is also used to store all tagged packets.) The default values are listed in Table 3.

Table 3. Default Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0 or 1	Q0 (lowest)
2 or 3	Q1
4 or 5	Q2
6 or 7	Q3 (highest)

- If you are configuring a tagged port and you want the port to ignore the priority tag in egress tagged packets, click the **Override Priority** option. A check in the box indicates this feature is activated. All tagged packets are directed to the egress queue specified in Step 6.

Note

The tagged information in a packet is not changed as the packet traverses the switch. A tagged packet exits the switch with the same priority level that it had when it entered.

The default for this parameter is No, meaning that the priority level of tagged packets is determined by the priority level specified in the packet itself.

7. Click **Apply**.

Configuration changes are immediately activated on the switch.

8. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues, as shown in Table 3 on page 143. This is set at the switch level. You cannot set this on a per-port basis.

To change the mappings, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **QoS** option.

The QoS page is displayed with the CoS tab selected by default, as shown in Figure 40 on page 142.

3. Select the **Scheduling** tab.

The Scheduling tab is shown in Figure 42.

The screenshot shows the 'Configuration' page of a network device. At the top, there's a header with 'AT-9424T/SP' and a yellow 'Configuration' banner. Below the banner, system information is displayed: 'System Name: Marketing' and 'MAC Addr: 00:30:84:00:00:00'. A left sidebar contains navigation buttons: Home, System, Layer 1, Layer 2, Security, QoS (highlighted), Help, and Logout. The main content area has two tabs: 'CoS' and 'Scheduling' (selected). Under the 'Scheduling' tab, there are two sections: 'Configure CoS Priority to Egress Queues' and 'Configure Egress Weights'. The first section contains two columns of dropdown menus for mapping CoS priorities (0-7) to egress queues (PQ 0-7). The second section, 'Configure Egress Weights', includes a 'Select Schedule' radio button group (Strict Priority is selected) and eight input fields for queue weights (0-7), each with a range of [0 - 15]. An 'Apply' button is at the bottom right.

Figure 42. QoS Scheduling Tab (Configuration)

Note

The Configure Egress Weights section in the tab is explained in the next procedure, "Configuring Egress Scheduling" on page 148.

4. In the Configure CoS Queues to Egress Queues section of the tab, click the list for a CoS priority whose queue assignment you want to change and select the new queue.

For example, to direct all tagged packets with a CoS priority of 5 to egress queue Q3, you would use the list in **CoS 5 to PQ** and select **Q3 - QoS PriorityQ 3**.

5. If desired, repeat Step 4 to change the egress queue assignment of other CoS priorities.
6. Click **Apply**.

7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Configuring Egress Scheduling

This procedure explains how to select and configure a scheduling method for QoS. Scheduling determines the order in which the ports handle packets in their egress queues. For an explanation of the two scheduling methods, refer to “Scheduling” in Chapter 13, “Quality of Service,” in the *AT-S63 Management Software Menus Interface User’s Guide*. Scheduling is set at the switch level. You cannot set this at the port level.

To change scheduling, perform the following procedure:

- 1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

- 2. From the Configuration menu, select the **QoS** option.

The QoS page is displayed with the CoS tab selected by default, as shown in Figure 40 on page 142.

- 3. Select the **Scheduling** tab.

The Scheduling tab is shown in Figure 42 on page 146.

Note

The Configure CoS Queues to Egress Queues section in the tab is explained in the previous procedure “Mapping CoS Priorities to Egress Queues” on page 145.

- 4. To select a scheduling method, click either **Strict Priority** or **Weighted Priority** in the Configure Egress Weights section of the tab. The default is Strict Priority.

Skip the next step if you select Strict Priority. Queue weights do not apply to Strict Priority scheduling.

- 5. If you selected Weighted Priority, use the Queue # Weight fields to specify for each queue the number of packets you want a port to transmit before it goes to the next queue. For an example, refer to Table 4.

Table 4. Example of Weighted Round Robin Priority

Port Egress Queue	Maximum Number of Packets
Q3	15

Table 4. Example of Weighted Round Robin Priority (Continued)

Port Egress Queue	Maximum Number of Packets
Q2	10
Q1	5
Q0	1

Leaving the default value of 1 for each queue results in all egress queues being given the same priority.

6. Click **Apply**.
7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying the CoS Settings

To display the CoS settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44

2. From the Monitoring menu, select the **QoS** option.

The QoS page is displayed with the CoS tab selected by default, as shown in Figure 43.

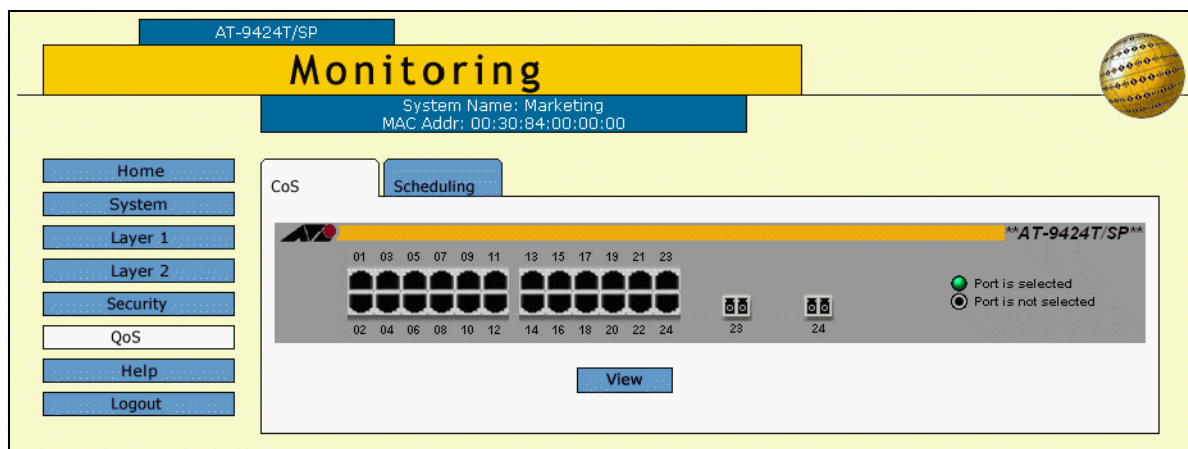


Figure 43. CoS Tab (Monitoring)

3. Click the port where you want to view the settings. You can select more than one port at a time. A selected port turns white. (To deselect a port, click it again.)
4. Click **View**.

The CoS Setting for Port page is shown in Figure 44.

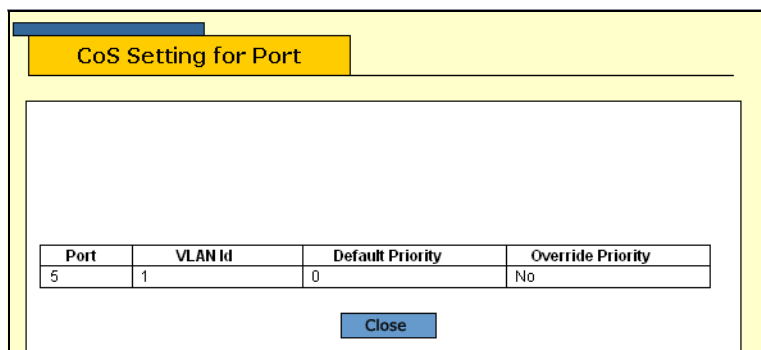


Figure 44. CoS Setting for Port Page

The CoS Setting for Port page displays a table that contains the following columns of information:

Port

The port number.

VLAN ID

The VLAN of which the port is a member.

Default Priority

The default priority level for this port.

Override Priority

Whether or not the default priority should be overridden.

Displaying the QoS Schedule

To display the QoS schedule, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44

2. From the Monitoring menu, select the **QoS** option.

The QoS page is displayed with the CoS tab selected by default, as shown in Figure 43 on page 150.

3. Select the **Scheduling** tab.

The Scheduling tab is shown in Figure 45.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

CoS Scheduling

CoS Priority to Egress Queues

CoS 0 to PQ QoS PriorityQ 0	CoS 1 to PQ QoS PriorityQ 1
CoS 2 to PQ QoS PriorityQ 2	CoS 3 to PQ QoS PriorityQ 3
CoS 4 to PQ QoS PriorityQ 4	CoS 5 to PQ QoS PriorityQ 5
CoS 6 to PQ QoS PriorityQ 6	CoS 7 to PQ QoS PriorityQ 7

Egress Weights

Select Schedule Strict Priority	
Queue 0 Weight(Weighted) Weight 0	Queue 4 Weight(Weighted) Weight 0
Queue 1 Weight(Weighted) Weight 0	Queue 5 Weight(Weighted) Weight 0
Queue 2 Weight(Weighted) Weight 0	Queue 6 Weight(Weighted) Weight 0
Queue 3 Weight(Weighted) Weight 0	Queue 7 Weight(Weighted) Weight 0

Figure 45. QoS Scheduling Tab (Monitoring)

The upper section displays the CoS priority to egress queue assignments. The lower section displays the egress weight settings.

Chapter 13

IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch. The sections in the chapter include:

- ❑ "Configuring IGMP Snooping" on page 154
- ❑ "Displaying a List of Host Nodes" on page 157
- ❑ "Displaying a List of Multicast Routers" on page 160

Note

For background information, refer to Chapter 14, "IGMP Snooping," in the *AT-S63 Management Software Menus Interface User's Guide*.

Configuring IGMP Snooping

To configure IGMP snooping, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40

2. Select the **IGMP** tab.

The IGMP tab is shown in Figure 46.

Figure 46. IGMP Tab (Configuration)

3. Adjust the following parameters as necessary.

Enable IGMP Snooping Status

Enables and disables IGMP snooping on the switch. A check in the box indicates that IGMP is enabled.

Multicast Host Topology

Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

The Edge (Single-Host/Port) setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending reports and times out. The switch

forwards the leave request to the router and simultaneously ceases transmission of any further multicast packets out the port where the host node is connected.

The Intermediate (Multi-Host) setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port continue to receive the multicast packets. Only after all of the host nodes connected to a switch port have transmitted leave requests (or have timed out) does the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Intermediate Multi-Host Port selection.

Multicast Router Ports Mode

Specifies whether the router ports are determined automatically or if you enter them manually. If you want the switch to determine the ports automatically, select Auto-Detect, which is the default. To enter them yourself, click Manual Select and enter the ports in the field.

Host/Router Timeout Interval

Specifies the time period in seconds after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

Maximum Multicast Groups

Specifies the maximum number of multicast groups the switch learns. The range is 1 to 255 groups. The default is 64 multicast groups.

This setting is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast

addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

4. Click **Apply**.
5. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying a List of Host Nodes

You can use the AT-S63 management software to display a list of the multicast groups on a switch, as well as the host nodes. You can also view the multicast routers. A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes.

To view host nodes, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **IGMP** tab.

The IGMP tab is shown in Figure 47.

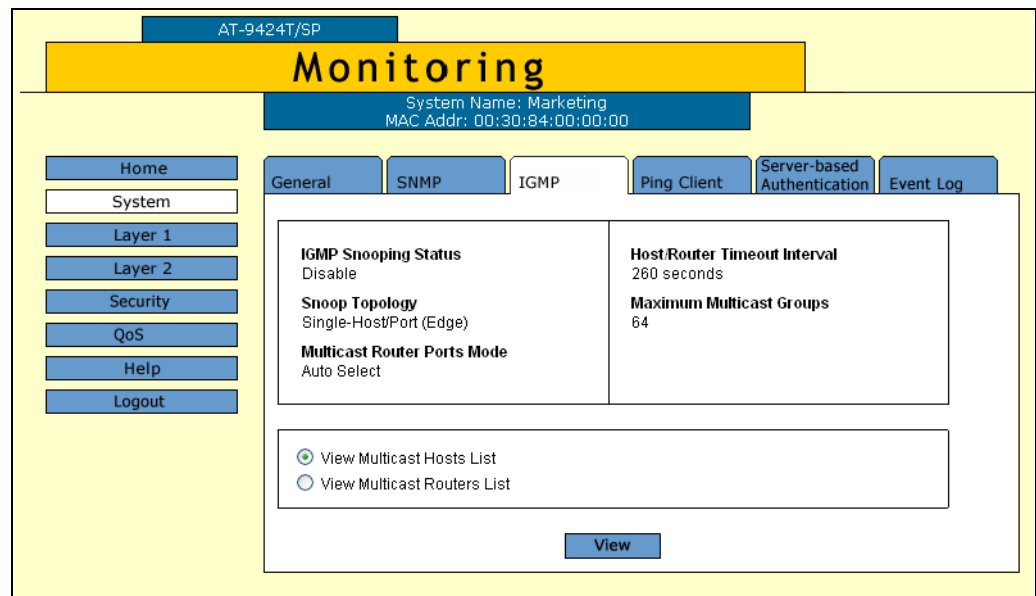


Figure 47. IGMP Tab (Monitoring)

The IGMP tab provides the following information:

Enable IGMP Snooping Status

The IGMP snooping status on the switch. Possible settings are Enabled and Disabled

Snoop Topology

Whether there is only one host node per switch port or multiple host nodes per port. The possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

Multicast Router Ports Mode

How the router ports are determined. The possible settings are:

Auto-Detect - The switch determines the ports automatically.

Port number - The selected router ports.

Host/Router Timeout Interval

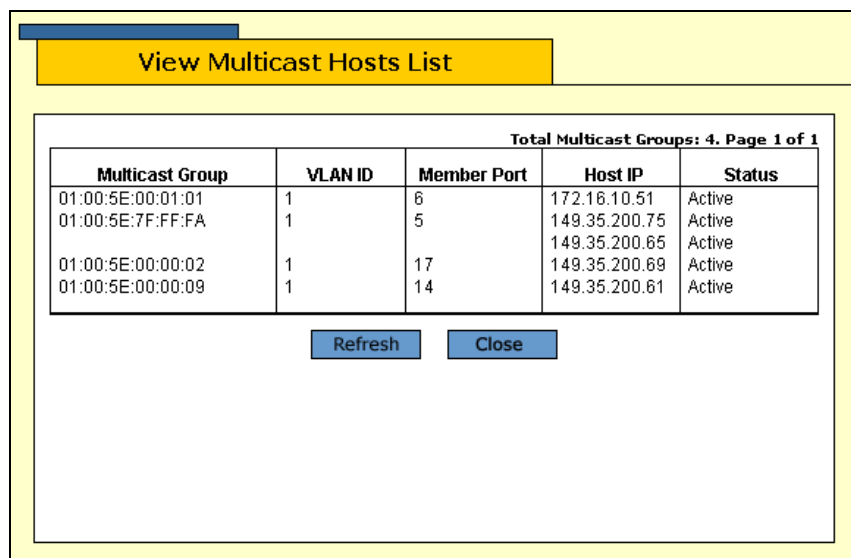
The time period in seconds after which the switch determines that a host node has become inactive.

Maximum Multicast Groups

The maximum number of multicast groups the switch learns.

- To view the multicast addresses and the host nodes, click **View Multicast Hosts List** and then click **View**.

The View Multicast Hosts List is shown in Figure 48.



Total Multicast Groups: 4. Page 1 of 1				
Multicast Group	VLAN ID	Member Port	Host IP	Status
01:00:5E:00:01:01	1	6	172.16.10.51	Active
01:00:5E:7F:FF:FA	1	5	149.35.200.75	Active
			149.35.200.65	Active
01:00:5E:00:00:02	1	17	149.35.200.69	Active
01:00:5E:00:00:09	1	14	149.35.200.61	Active

Refresh Close

Figure 48. View Multicast Hosts List Page

The View Multicast Hosts List page displays a table that contains the following columns of information:

Multicast Group

The multicast address of the group.

VLAN ID

The VID of the VLAN in which the port is an untagged member.

Member Port

The port(s) on the switch to which one or more host nodes of the multicast group are connected.

Host IP

The IP address(es) of the host node(s) connected to the port.

Status

Indicates IGMP group status of the port. The possible settings are:

Active - The port is active in the IGMP group.

Left Group - The port is not active in the IGMP group.

Displaying a List of Multicast Routers

To view multicast routers, perform the following procedure:

1. From the Home page, select **Monitoring**.

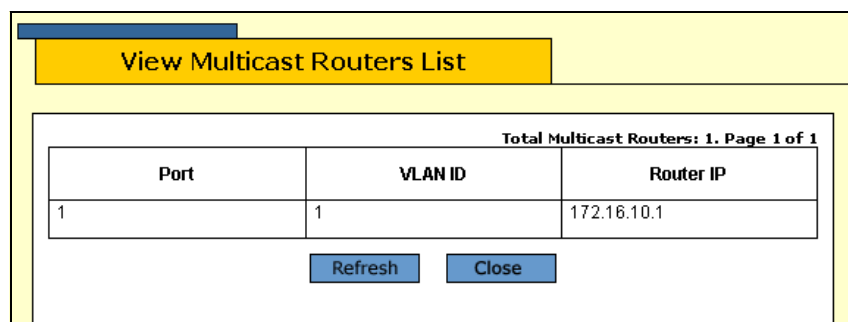
The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **IGMP** tab.

The IGMP tab is shown in Figure 47 on page 157.

3. To view the multicast routers, click **View Multicast Router List** and then click **View**.

The View Multicast Routers List is shown in Figure 49.



Total Multicast Routers: 1. Page 1 of 1		
Port	VLAN ID	Router IP
1	1	172.16.10.1

Refresh Close

Figure 49. View Multicast Routers List Page

The View Multicast Routers List page displays a table that contains the following columns of information:

Port

The port on the switch where the multicast router is connected.

VLAN ID

The VID of the VLAN in which the port is an untagged member.

Router IP

The IP address of the port on the router.

If the routers are static routers (specified with the Manual Select option on the Configuration IGMP page), then the View Multicast Routers List page opens, as shown in Figure 50.

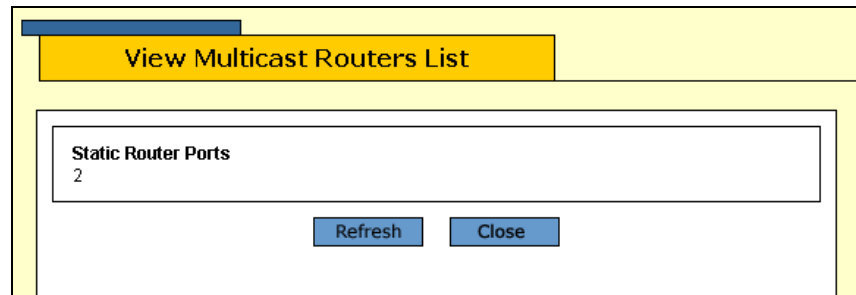


Figure 50. View (Static) Multicast Routers List Page

Chapter 14

STP and RSTP

This chapter explains how to configure the STP and RSTP parameters on an AT-9400 Series switch. The sections in the chapter include:

- ❑ "Enabling or Disabling a Spanning Tree Protocol" on page 164
- ❑ "Configuring STP" on page 166
- ❑ "Configuring RSTP" on page 174

Note

For background information on spanning tree, refer to Chapter 16, "STP and RSTP," in the *AT-S63 Management Software Menus Interface User's Guide*.

Multiple Spanning Tree Protocol (MSTP) is described in Chapter 15, "MSTP" on page 181.

Enabling or Disabling a Spanning Tree Protocol

To enable or disable spanning tree on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51.

Figure 51. Spanning Tree Tab (Configuration)

4. To enable or disable spanning tree, click the **Enable Spanning Tree** check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.
5. To select a spanning tree version, for the Active Protocol Version parameter click **STP**, **RSTP**, or **MSTP**. The default is RSTP.

Note

Only one spanning tree protocol can be active on the switch at a time.

6. Click **Apply**.

7. If you activated STP, go to "Configuring STP" on page 166. If you activated RSTP go to Step "Configuring RSTP" on page 174. If you activated MSTP, go to Chapter 15, "MSTP" on page 181.

Configuring STP



Caution

The bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

To configure STP, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The Configure STP Parameters tab is shown in Figure 52.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

MAC Address VLAN GVRP Spanning Tree Enhanced Stacking

Configure STP Parameters

Bridge Priority [0-15] <input type="text" value="8"/> * 4096 = 32768 Bridge Hello Time [1-10] <input type="text" value="2"/> Bridge Forwarding [4-30] <input type="text" value="15"/>	Bridge Max Age [6-40] <input type="text" value="20"/> Bridge Identifier 00:30:84:00:00:00
---	--

Apply Defaults

AT-9424T/SP
 Port is active
 Port is inactive
 Port is disabled
 Port is selected

Modify Back

Figure 52. Configure STP Parameters Tab (Configuration)

Note

The Defaults button returns all STP settings to the default settings.

- Adjust the following parameters as necessary.

Bridge Priority

The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This

parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 5.

Table 5. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Bridge Hello Time

The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Forwarding Delay

The waiting period in seconds before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.

Bridge Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds.

In selecting a value for maximum age, the following rules must be observed:

MaxAge must be greater than $(2 \times (\text{HelloTime} + 1))$

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

Note

The aging time for BPDUs is different from the aging time used by the MAC address table.

Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

6. After you have made the desired changes, click **Apply**.
7. To adjust a port's STP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

The STP Settings - Port(s) page is shown in Figure 53.

Figure 53. STP Settings - Port(s) Page

8. Adjust the following parameters as necessary.

Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to Table 6.

Table 6. Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176

Table 6. Port Priority Value Increments (Continued)

Increment	Bridge Priority	Increment	Bridge Priority
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 65,535. The default setting is Auto-detect, which sets port cost depending on the speed of the port. If you select Auto-Detect, the management software assigns a value of 100 if the port is operating at 10 Mbps, 10 for 100 Mbps, and 4 for one gigabit.

9. After you have configured the parameters, click **Apply**.
10. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Note

A change to the port priority parameter takes effect immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Displaying the STP Settings

To display the STP settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 54.

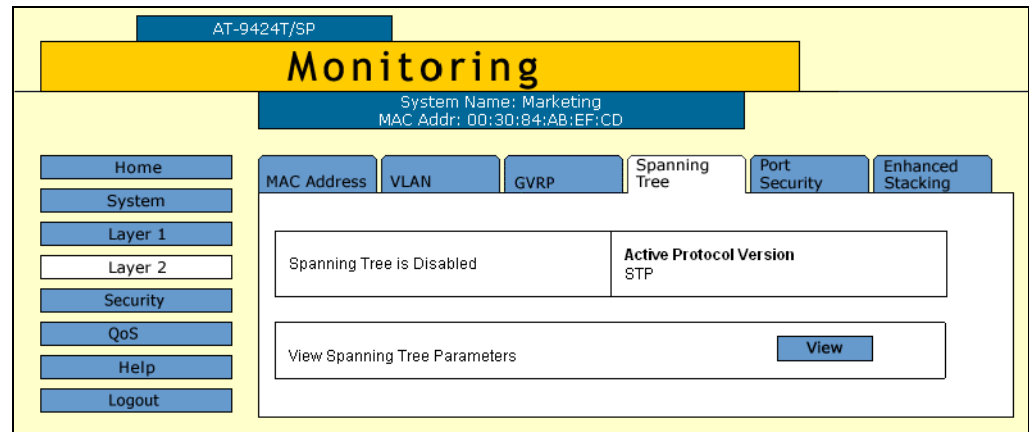


Figure 54. Spanning Tree Tab (Monitoring)

4. Click **View**.

The Monitor STP Parameters tab is shown in Figure 55.

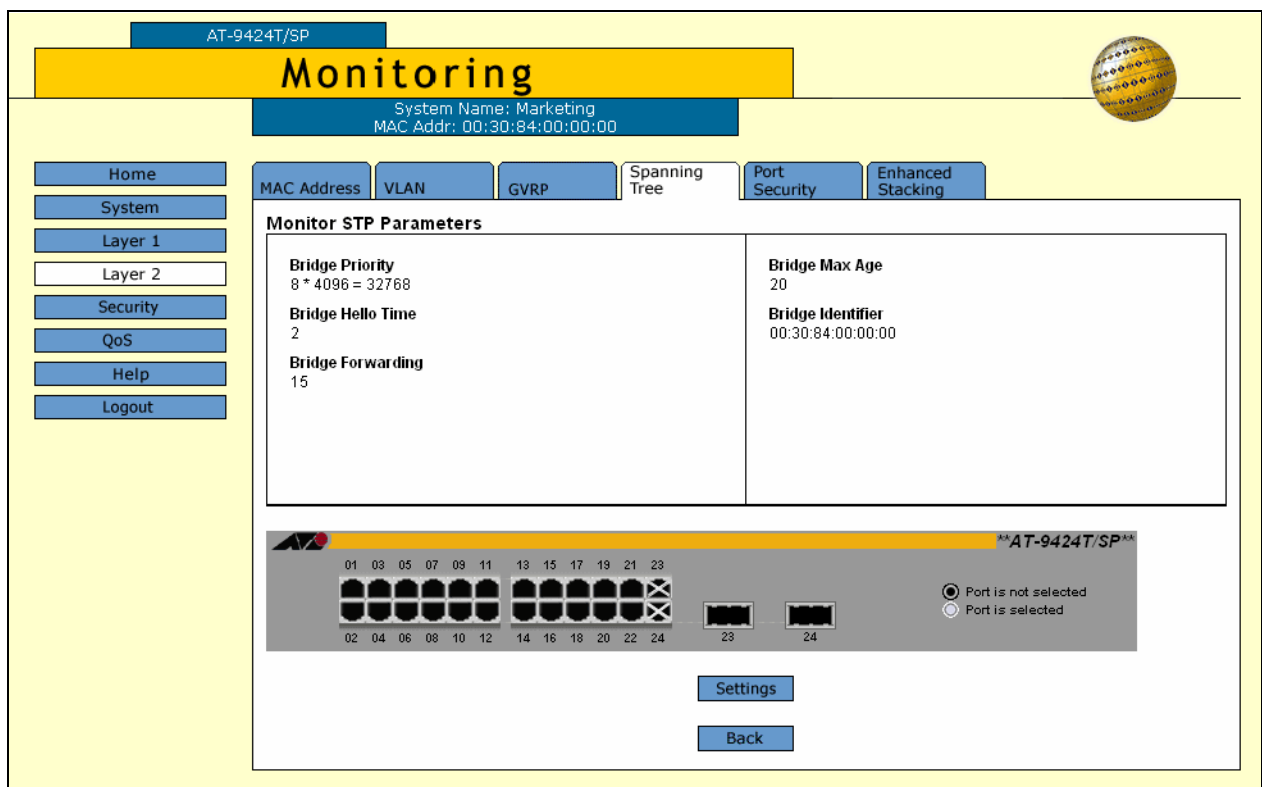


Figure 55. Monitor STP Parameters Tab (Monitoring)

5. To view port settings, click a port in the switch and click **Status** or **Settings**.

The STP Settings page is shown in Figure 56.

Port	State	Cost	Priority
15	Disabled	--	128

OK

Figure 56. STP Settings Page

The STP Settings page displays a table that contains the following columns of information:

Port

Port number.

State

Current state of the port. The possible states are Enabled or Disabled.

Cost

Port cost of the port. The default is Auto-Update.

Priority

The number used as a tie-breaker when two or more ports have equal costs to the root bridge.

6. Click **OK** to close the page.

Resetting STP to the Default Settings

To reset STP to the factory default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The Configure STP Parameters tab is shown in Figure 52 on page 167.

5. Click **Defaults**.

The STP defaults are shown in "STP, RSTP, and MSTP Default Settings" on page 369.

Configuring RSTP



Caution

The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

To configure RSTP, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The Configure RSTP Bridge Parameters tab is shown in Figure 57.

The screenshot displays the 'Configuration' page for an AT-9424T/SP device. The top header shows the system name 'Marketing' and MAC address '00:30:84:00:00:00'. The left navigation menu includes links for Home, System, Layer 1, Layer 2, Security, QoS, Help, and Logout. The main configuration area is titled 'Configure RSTP Parameters' and includes tabs for MAC Address, VLAN, GVRP, Spanning Tree, and Enhanced Stacking. The 'Spanning Tree' tab is active, showing the following parameters:

- Force Version:** Radio buttons for 'Force STP Compatible' and 'RSTP' (selected).
- Bridge Priority [0-15]:** Input field '8' with a calculation '* 4096 = 32768'.
- Bridge Hello Time [1-10]:** Input field '2'.
- Bridge Forwarding [4-30]:** Input field '15'.
- Bridge Max Age [6-40]:** Input field '20'.
- Bridge Identifier:** '00:30:84:00:00:00'.

Below the configuration fields are 'Apply' and 'Defaults' buttons. At the bottom, there is a port configuration section with a grid of 24 ports (01-24) and a legend indicating 'Port is not selected' (radio button) and 'Port is selected' (radio button). A 'Modify' button is located below the port grid, and a 'Back' button is at the bottom right.

Figure 57. Configure RSTP Parameters Tab (Configuration)

- Adjust the following parameters as necessary.

Force Version

This selection determines whether the bridge operates with RSTP or in an STP-compatible mode. If you select RSTP, the bridge operates all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge operates in RSTP, using the RSTP parameter settings, but it sends only STP BPDU packets out the ports.

Bridge Priority

The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 5 on page 168.

Bridge Hello Time

The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Forwarding

The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Bridge Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than $(2 \times (\text{HelloTime} + 1))$.

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

6. After you have made your changes, click **Apply**.
7. To adjust RSTP port settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

The RSTP Settings - Port(s) page is shown in Figure 58.

Figure 58. RSTP Settings - Port(s) Page

8. Adjust the following parameters as necessary.

Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to Table 6 on page 169.

Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20,000,000. The default setting is Automatic detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 16, "STP and RSTP" in the *AT-S63 Management Software Menus Interface User's Guide*.

Edge Port

This parameter defines whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 16, "STP and RSTP" in the *AT-S63 Management Software Menus Interface User's Guide*.

9. After you have configured the parameters, click **Apply**.

10. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Note

All changes to a port's RSTP settings, with the exception of port cost, are activated immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Resetting RSTP to the Default Settings

To reset RSTP to the default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select **Layer 2**.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The Configure RSTP Bridge Parameters tab is shown in Figure 57 on page 175.

5. Click **Defaults**.

The RSTP defaults are shown in "STP, RSTP, and MSTP Default Settings" on page 369.

Displaying RSTP Settings

To display RSTP parameter settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is displayed, as shown in Figure 54 on page 171.

This tab displays information on whether spanning tree is enable or disabled and which protocol version, STP or RSTP, is active.

4. Click **View**.

The Monitor RSTP Parameters tab is shown in Figure 59.

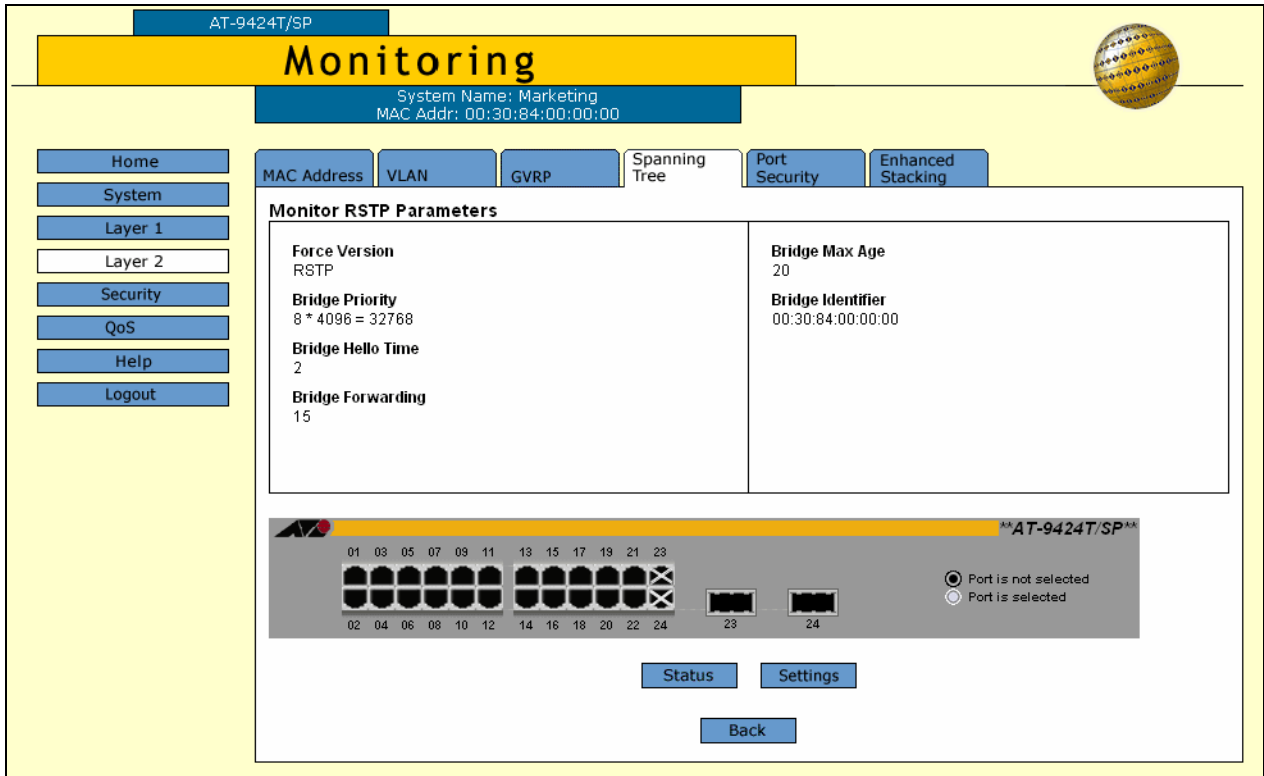


Figure 59. Monitor RSTP Parameters Tab (Monitoring)

5. To view port settings, click a port in the switch and click **Status** or **Settings**.

The RSTP Settings page is shown in Figure 60.

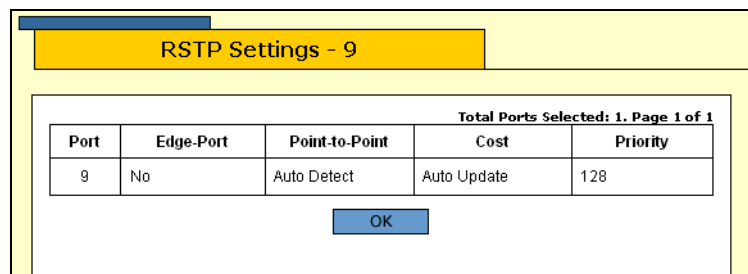


Figure 60. RSTP Settings Page

The RSTP Settings page displays a table that contains the following columns of information:

Port

The port number.

Edge-Port

Whether or not the port is operating as an edge port. The possible settings are Yes and No.

Point-to-Point

Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto Detect.

Cost

Port cost of the port. The default is Auto Update.

Priority

The number used as a tie-breaker when two or more ports have equal costs to the root bridge.

6. Click **OK** to close the page.

Chapter 15

MSTP

This chapter explains how to configure MSTP parameters on an AT-9400 Series switch using a web browser management session. It contains the following procedures:

- ❑ "Enabling MSTP" on page 182
- ❑ "Configuring MSTP" on page 184
- ❑ "Creating, Deleting, or Modifying MSTI IDs" on page 189
- ❑ "Adding, Removing, or Modifying VLAN Associations to MSTIs" on page 192
- ❑ "Configuring MSTP Port Parameters" on page 195
- ❑ "Displaying the MSTP Port Configuration" on page 197
- ❑ "Displaying the MSTP Port Status" on page 200
- ❑ "Displaying the MSTP Port Status" on page 200
- ❑ "Resetting MSTP to the Default Settings" on page 202

Note

For background information on STP and RSTP, refer to Chapter 16, "STP and RSTP," in the *AT-S63 Management Software Menus Interface User's Guide*. For background information on MSTP, refer to Chapter 17, "MSTP," in the *AT-S63 Management Software Menus Interface User's Guide*.

Enabling MSTP

The AT-9400 Series switch can support the three spanning tree protocols STP, RSTP, and MSTP. However, only one spanning tree protocol can be active on the switch at a time. So before you can enable a spanning tree protocol, you must first select it as the active spanning tree protocol. After you select it, you can then enable or disable it.

To select MSTP as the active spanning tree protocol and to enable or disable it, perform the following procedure:

Note

Changing the active spanning tree protocol resets the switch.

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 61.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

MAC Address VLAN GVRP Spanning Tree Enhanced Stacking

☐ Enable Spanning Tree

Active Protocol Version
☒ STP ☐ RSTP ☐ MSTP

Apply

Configure Spanning Tree Parameters Configure

Figure 61. Spanning Tree Tab (Configuration)

Note

If you do not want to change the active spanning tree protocol and just want to enable or disable it, go to Step 5.

4. To change the active spanning tree protocol on the switch, click **STP**, **RSTP**, or **MSTP** in the Active Protocol Version section of the tab. The default is RSTP.

Note

Only one spanning tree protocol can be active on the switch at a time.

5. To enable or disable the active spanning tree protocol on the switch, click the **Enable Spanning Tree** check box. A check indicates that the spanning tree is enabled while no check indicates that spanning tree is disabled. The default is disabled.
6. Click **Apply**.

Note

If you changed the active spanning tree protocol, the switch resets and your management session is ended. To continue managing the switch, you must restart your management session after the switch is finished reloading the AT-S63 management software.

7. If you activated STP, go to "Configuring STP" on page 166. If you activated RSTP go to "Configuring RSTP" on page 174. If you activated MSTP, go to "Configuring MSTP" on page 184.

Configuring MSTP

This section contains the following procedures:

- ❑ "Configuring MSTP Parameters" on page 184
- ❑ "Configuring the CIST Priority" on page 187
- ❑ "Creating, Deleting, or Modifying MSTI IDs" on page 189
- ❑ "Adding, Removing, or Modifying VLAN Associations to MSTIs" on page 192
- ❑ "Configuring MSTP Port Parameters" on page 195

Note

MSTP must be selected as the active spanning tree protocol on the switch before you can configure it. For instructions on selecting the active spanning tree, refer to "Enabling MSTP" on page 182.

Note

When MSTP is enabled, the GVRP tab is not shown on the Configuration or Monitoring Layer 2 page.

Configuring MSTP Parameters

To configure MSTP parameters, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

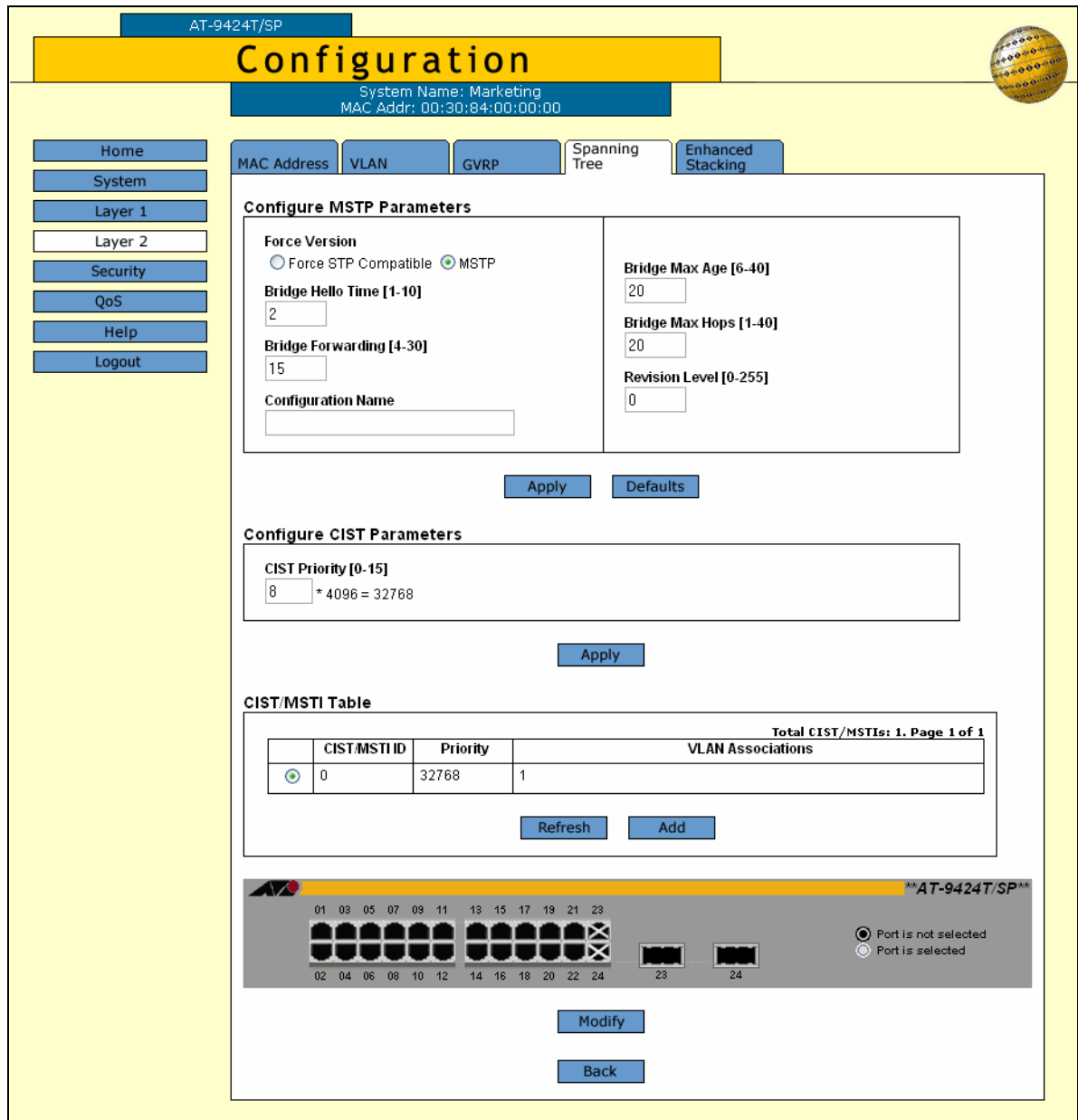
The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62.



AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

MAC Address VLAN GVRP Spanning Tree Enhanced Stacking

Configure MSTP Parameters

Force Version
☐ Force STP Compatible ☒ MSTP

Bridge Hello Time [1-10]

Bridge Forwarding [4-30]

Configuration Name

Bridge Max Age [6-40]

Bridge Max Hops [1-40]

Revision Level [0-255]

Apply Defaults

Configure CIST Parameters

CIST Priority [0-15]
 * 4096 = 32768

Apply

CIST/MSTI Table

Total CIST/MSTIs: 1. Page 1 of 1

	CIST/MSTI ID	Priority	VLAN Associations
	0	32768	1

Refresh Add

AT-9424T/SP

01 03 05 07 09 11 13 15 17 19 21 23
 02 04 06 08 10 12 14 16 18 20 22 24

Port is not selected
 Port is selected

Modify Back

Figure 62. Configure MSTP Parameters Tab (Configuration)

Note

This procedure explains the Configure MSTP Parameters section of the page. The CIST/MSTI Table is explained in "Adding, Removing, or Modifying VLAN Associations to MSTIs" on page 192. The graphic image of the switch is described in "Configuring MSTP Port Parameters" on page 195.

Adjust the following parameters as necessary.

Force Version

This selection determines whether the bridge operates with MSTP or in an STP-compatible mode. If you select MSTP, the bridge operates all ports in MSTP, except those ports that receive STP or RSTP BPDU packets. If you select Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports. The default is MSTP.

Bridge Hello Time

The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds. This value is active only if the bridge is selected as the root bridge of the network.

Bridge Forwarding

The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all of the links may have adapted to the change, possibly resulting in a network loop. The range is from 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Configuration Name

The name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters in length. The name, which is case sensitive, must be the same on all bridges in a region. Examples of a configuration name include Sales Region and Production Region.

Bridge Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs.

All bridges in a single-instance bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than $(2 \times (\text{HelloTime} + 1))$

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

Bridge Max Hops

MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses an MSTP region boundary. After the counter reaches zero, the BPDU is deleted.

Revision Level

The revision level of an MSTP region. This is an arbitrary number that you assign to a region. The revision level must be the same on all bridges in a region. Different regions can have the same revision level without conflict. The range is 0 (zero) to 255.

5. Click **Apply**.
6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Or, proceed to the next procedure to configure the CIST priority.

Configuring the CIST Priority

To configure the CIST priority, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

5. In the Configure CIST Parameters section, set the **CIST Priority**, the priority number for the bridge.

This number is used to determine the root bridge of the bridged network. This number is analogous to the RSTP bridge priority value. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

6. Click **Apply**.
7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Creating, Deleting, or Modifying MSTI IDs

To create, delete, or modify MSTI IDs, perform one of the following procedures.

Creating an MSTI ID

To create an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

5. In the CIST/MSTI Table section of the tab, click **Add**.

The Add New MSTI page is shown in Figure 63.

Figure 63. Add New MSTI Page

6. In the MSTI ID field, enter a new MSTI ID. The range is 1 to 15.
7. In the Priority field, enter an MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. This

parameter is used in selecting a regional root for the MSTI. For a list of the increments, refer to Table 5, "Bridge Priority Value Increments" on page 168. The default is 0.

8. Click **Apply**.
9. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

10. Repeat this procedure to create more MSTI IDs.

Deleting an MSTI ID

To delete an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

5. In the CIST/MSTI Table section of the tab, click the button next to the MSTI ID you want to delete. You can select only one MSTI ID at a time.
6. Click **Remove**.
7. A confirmation prompt is displayed.
8. Click **OK** to delete the MSTI or **Cancel** to cancel the procedure:
9. If you select OK, the MSTI is deleted and VLANs associated with it are returned to CIST, which has an ID of 0.

Modifying an MSTI ID

To modify an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

- From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

- Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

- Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

- In the CIST/MSTI Table section of the tab, click the button next to the MSTI ID you want to modify. You can select only one MSTI ID at a time. You cannot modify CIST.

- Click **Modify**.

The Modify MSTI page is shown in Figure 64.

The screenshot shows a web browser interface for modifying an MSTI. The title bar is yellow and says "Modify MSTI". The main content area is white and contains a form with the following fields:

- MSTI ID**: 2
- Priority**: 7 * 4096 = 28672
- VLAN List**: 3

At the bottom of the form are two buttons: "Apply" and "Cancel".

Figure 64. Modify MSTI Page

- In the Priority field, enter a new MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. For a list of the increments, refer to Table 5, "Bridge Priority Value Increments" on page 168. The default is 0.
 - Click **Apply**.
 - To permanently save the change, return to the General tab on the System page and click **Save Changes**.
- For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.
- Repeat this procedure to modify more MSTI IDs.

Adding, Removing, or Modifying VLAN Associations to MSTIs

This section explains how to add or remove VLANs associated to MSTI IDs.

Adding a VLAN Association

To add a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, enter the VIDs of the VLANs to be associated with this MSTI. You can specify more than one VID at a time (for example, 2,4,7).

6. Click Apply.

7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Or, proceed to the next procedure to configure the CIST priority.

Removing a VLAN Association

To remove a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, remove the VIDs of the VLANs that you no longer want to be associated with this MSTI. You can specify more than one VID at a time (for example, 2,4,7).
6. Click Apply.
7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Or, proceed to the next procedure to configure the CIST priority.

Modifying a VLAN Association

To modify a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 164.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, modify the VIDs of the VLANs that you no longer want to be associated with this MSTI. You can specify more than one VID at a time (e.g., 2,4,7).
6. Click Apply.
7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to “Saving Your Parameter Changes” on page 36.

Configuring MSTP Port Parameters

To configure MSTP port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 61 on page 182.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

5. In the diagram of the switch at the bottom of the MSTP Spanning Tree Expanded page, click the ports you want to configure. You can select more than one port at a time.

6. Click **Modify**.

The MSTP Settings - Port(s) page is shown in Figure 65.

Figure 65. MSTP Settings - Port(s) Page

7. Adjust the following parameters as necessary.

Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge. The

range is 0 to 240 in increments of 16. The default value is 8 (priority value is 128). For a list of the increments, refer to Table 6, "Port Priority Value Increments" on page 169.

Port Internal Path Cost

The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Edge Port

This parameter defines whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 16, "STP and RSTP" in the *AT-S63 Management Software Menus Interface User's Guide*.

Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 16, "STP and RSTP" in the *AT-S63 Management Software Menus Interface User's Guide*.

Port External Path Cost

The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP. The range is 0 to 200,000,000. The default setting is 200,000.

8. After adjusting the parameters, click **Apply**.
9. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

10. Repeat this procedure to configure MSTP parameters for other switch ports.

Displaying the MSTP Port Configuration

To display the MSTP port configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Monitoring Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

The Monitor MSTP Parameters tab is shown in Figure 66.

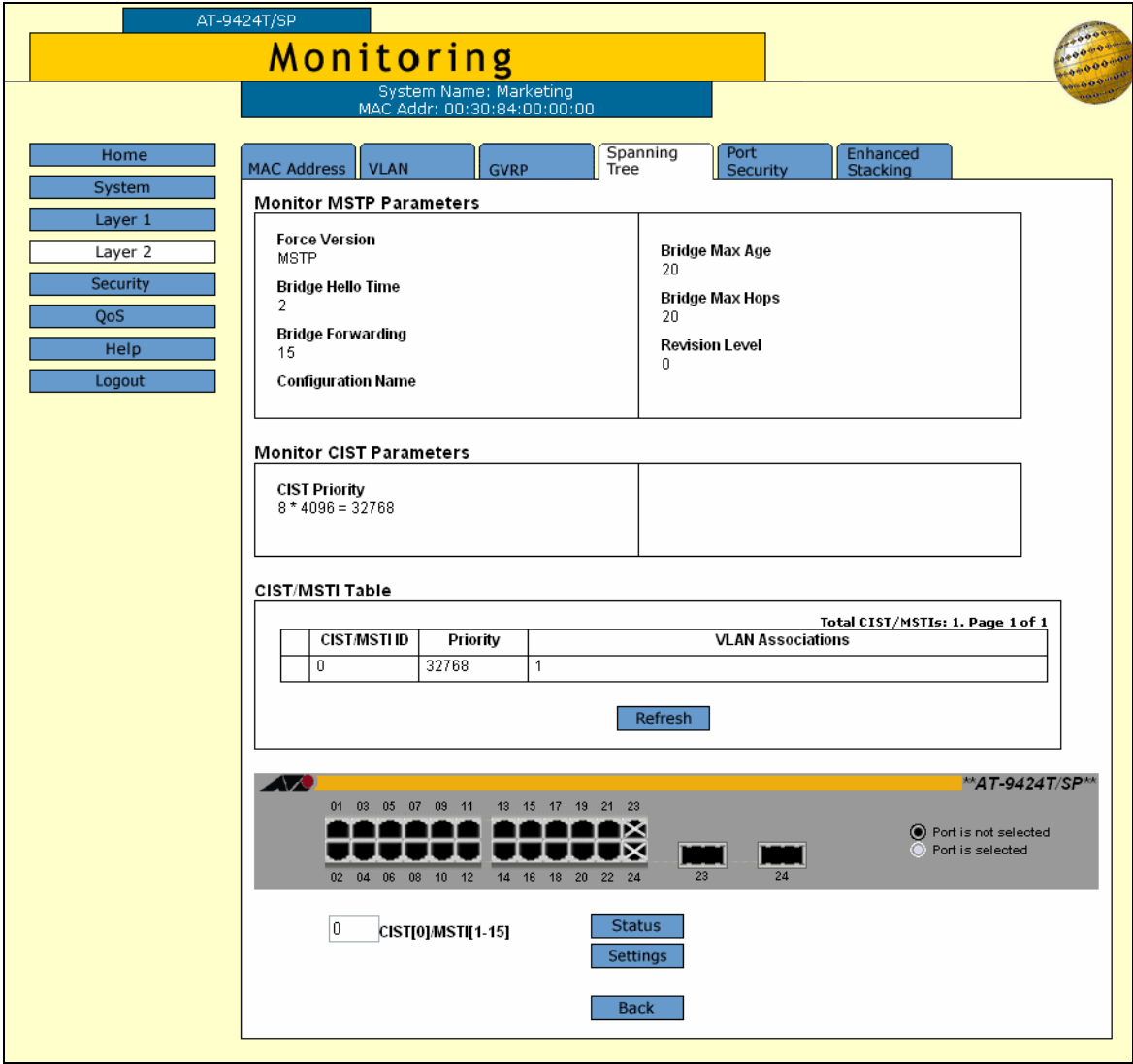


Figure 66. Monitor MSTP Parameters Tab (Monitoring)

- 4. Click a port in the switch and click **Settings**. You can select more than one port.

The MSTP Settings - Port (s) page is shown in Figure 67.

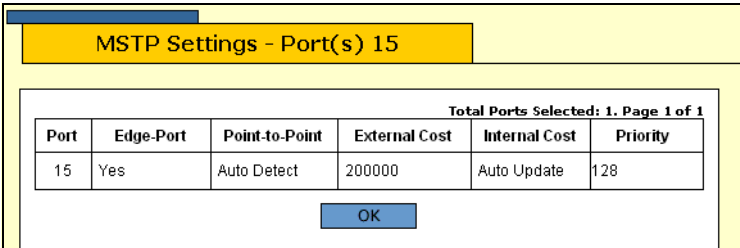


Figure 67. MSTP Settings - Port(s) Page

The MSTP Settings page displays a table that contains the following columns of information:

Port

The port number.

Edge-Port

Whether or not the port is functioning as an edge port. The possible settings are Yes and No.

Point-to-Point

Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

External Cost

The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP.

Internal Cost

The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The possible settings are:

Auto-detect - Port cost is automatically set depending on the speed of the port.

Default values - 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge.

5. Click **OK** to close the page.

Displaying the MSTP Port Status

To display MSTP port status, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Monitoring Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

The Monitoring Spanning Tree tab for the active protocol, MSTP, is shown in Figure 66

4. Click a port in the switch and click **Status**. You can select more than one port.

The MSTP Port Status - Port(s) page is shown in Figure 68.

MSTP Port Status - Port(s) 17						
Total Ports Selected: 1. Page 1 of 1						
Port	State	CIST/MSTID	Role	P2P	Version	Port Cost
17	Disabled	0	---	---	---	---

OK

Figure 68. MSTP Port Status - Port(s) Page

The MSTP Port Status page displays a table that contains the following columns of information:

Port

The port number.

State

The MSTP state of the port. The possible states are:

Discarding - The port is discarding received packets and is not submitting forwarded packets for transmission.

Learning - The port is enabled for receiving, but not forwarding packets.

Forwarding - Normal operation.

Disabled - The port has not established a link with its end node.

Role

The MSTP role of the port. The possible roles are:

Root - The port that is connected to the root switch, directly or through other switches, with the least path cost.

Alternate - The port offers an alternate path in the direction of the root switch.

Backup - The port on a designated switch that provides a backup for the path provided by the designated port.

Designated - The port on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch.

Master - Similar to the root port. When the port is a boundary port, the MSTI port roles follow the CIST port roles. The MSTI port role is called "master" when the CIST role is "root."

P2P

Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

Version

Whether the port is operating in MSTP mode or STP-compatible mode.

Internal Port Cost

The port cost when the port is connected to a bridge in the same MSTP region.

5. Click **OK** to close the page.

Resetting MSTP to the Default Settings

To reset MSTP to the factory default settings, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 61 on page 182.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 62 on page 185.

5. Click **Defaults**.

The MSTP defaults are shown in "STP, RSTP, and MSTP Default Settings" on page 369.

Chapter 16

SNMPv3

This chapter provides the following procedures for configuring SNMPv3 parameters using a web browser management session:

- ❑ "Configuring the SNMPv3 Protocol" on page 204
- ❑ "Enabling or Disabling SNMP Management" on page 205
- ❑ "Configuring the SNMPv3 User Table" on page 207
- ❑ "Configuring the SNMPv3 View Table" on page 214
- ❑ "Configuring the SNMPv3 Access Table" on page 220
- ❑ "Configuring the SNMPv3 SecurityToGroup Table" on page 227
- ❑ "Configuring the SNMPv3 Notify Table" on page 233
- ❑ "Configuring the SNMPv3 Target Address Table" on page 238
- ❑ "Configuring the SNMPv3 Target Parameters Table" on page 245
- ❑ "Configuring the SNMPv3 Community Table" on page 252
- ❑ "Displaying SNMPv3 Tables" on page 258

Configuring the SNMPv3 Protocol

To configure the SNMPv3 protocol, you need to first enable SNMP access on the switch. Then you configure the SNMPv3 tables. See the following procedures:

- ☐ "Enabling or Disabling SNMP Management" on page 205
- ☐ "Configuring the SNMPv3 User Table" on page 207
- ☐ "Configuring the SNMPv3 View Table" on page 214
- ☐ "Configuring the SNMPv3 Access Table" on page 220
- ☐ "Configuring the SNMPv3 SecurityToGroup Table" on page 227
- ☐ "Configuring the SNMPv3 Notify Table" on page 233
- ☐ "Configuring the SNMPv3 Target Address Table" on page 238
- ☐ "Configuring the SNMPv3 Target Parameters Table" on page 245
- ☐ "Configuring the SNMPv3 Community Table" on page 252

Note

Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesyn does not recommend this configuration.

For reference information about the SNMPv3 protocol, see Chapter 18, "SNMPv3," in the *AT-S63 Management Software Menus Interface User's Guide*.

Enabling or Disabling SNMP Management

In order to allow an SNMP manager or host to access the switch you need to enable SNMP access. In addition, to allow the switch to send a trap when it receives a login attempt from an unauthenticated user, you need to enable authentication failure traps. This section provides a procedure to accomplish both of these tasks.

To enable SNMP access and authentication failure traps, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69.

The screenshot shows the 'Configuration' page for device 'AT-9424T/SP'. The 'System Name' is 'Marketing' and the 'MAC Addr' is '00:30:84:AB:EF:CD'. The left sidebar contains navigation links: Home, System, Layer 1, Layer 2, Security, QoS, Help, and Logout. The main content area has tabs for General, SNMP, IGMP, System Utilities, Server-based Authentication, and Event Log. The 'SNMP' tab is active, displaying two sections: 'Enable SNMP Access' and 'Enable Authentication Failure Trap', both with checkboxes and an 'Apply' button. Below these are sections for 'SNMPv1/v2c' (with a 'Configure' button) and 'SNMPv3' (showing the 'SNMP Engine ID' as '80:00:00:CF:03:00:30:84:AB:EF:CD' and a list of configuration options: 'Configure User Table' (selected), 'Configure View Table', 'Configure Access Table', 'Configure SecurityToGroup Table', 'Configure Notify Table', 'Configure Target Address Table', 'Configure Target Parameters Table', and 'Configure Community Table', with a 'Configure' button at the bottom).

Figure 69. SNMP Tab (Configuration)

3. Click the **Enable SNMP Access** checkbox to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the switch can be managed from an SNMP management station. No check indicates that the feature is disabled. The default is disabled.

Use this parameter to enable the switch to be remotely managed with an SNMP application program.

Note

If the Enable SNMP Access check box is not checked, the switch cannot be managed through SNMP. This is the default.

4. If you want the switch to send authentication failure traps, click the **Enable Authentication Failure Traps** checkbox. A check in the box indicates that the switch sends the trap.
5. Click **Apply**.
6. To save your changes, return to the General tab and click **Save Changes**.

Configuring the SNMPv3 User Table

You can create, delete, and modify an SNMPv3 User Table entry. See the following procedures:

- ❑ "Creating a User Table Entry" on page 207
- ❑ "Deleting a User Table Entry" on page 210
- ❑ "Modifying a User Table Entry" on page 211

For reference information about the SNMPv3 User Table, see Chapter 18, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a User Table Entry

To create an entry in the SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.
The Configuration System page is displayed with the General tab selected by default, as shown in Figure 69 on page 205.
2. Select the **SNMP** tab.
The SNMP tab is shown in Figure 69 on page 205.
3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 User Table tab is shown in Figure 70.

The screenshot shows the 'Configuration' page for an AT-9424T/SP device. The 'SNMP' tab is selected, and the 'SNMPv3 User Table' is displayed. The table lists four users: diane, jenny, chitra, and debashis. The 'Total Entries: 4. Page 1 of 1' is shown at the top right of the table. Below the table are buttons for 'Refresh', 'Add', 'Remove', 'Modify', and 'Back'.

	User Name	Authentication Protocol	Privacy Protocol	Storage Type	Row Status
<input checked="" type="radio"/>	diane	MD5	None	NonVolatile	Active
<input type="radio"/>	jenny	MD5	DES	NonVolatile	Active
<input type="radio"/>	chitra	SHA	DES	NonVolatile	Active
<input type="radio"/>	debashis	MD5	DES	NonVolatile	Active

Figure 70. SNMPv3 User Table Tab (Configuration)

4. Click **Add**.

The Add New SNMPv3 User page is shown in Figure 71.

The screenshot shows the 'Add New SNMPv3 User' page. It contains fields for Engine ID, User Name, Authentication Protocol, Authentication Password, Confirm Authentication Password, Privacy Protocol, Privacy Password, Confirm Privacy Password, Storage Type, and Row Status. The 'Apply' and 'Cancel' buttons are at the bottom.

Engine ID : 80:00:00:cf:03:00:30:84:fd:57:da
 User Name : chitra
 Authentication Protocol : SHA
 Authentication Password :
 Confirm Authentication Password :
 Privacy Protocol : DES
 Privacy Password :
 Confirm Privacy Password :
 Storage Type : NonVolatile
 Row Status : Active

Figure 71. Add New SNMPv3 User Page

- In the User Name field, enter a name, or logon id, that consists of up to 32 alphanumeric characters
- In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

Select one of the following:

MD5

This value represents the MD5 authentication protocol. With this selection, users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.

SHA

This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

None

This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

Note

You may want to assign NONE to a super user.

7. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.
8. In the Confirm Authentication Password field, re-enter the authentication password.

Note

If you have the nonencrypted version of the AT-S60 software, then the Privacy Protocol field is read-only.

Note

You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

9. In the Privacy Protocol field, enter one of the following options:

DES

Select this value to make the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

None

Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

10. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.
11. In the Confirm Privacy Password field, re-enter the privacy password.
12. In the Storage Type field, enter one of the following storage options for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the User Table. After making changes to an User Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the User Table. After making changes to an User Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 User Table.
14. To save your changes, return to the General tab and click **Save Changes**.

Deleting a User Table Entry

To delete an entry in the SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure**.

The SNMPv3 User Table tab is shown in Figure 70 on page 208.

- Click the button next to the User Table entry that you want to delete and then click **Remove**.

A warning message is displayed.

- Click **OK**.
- To save your changes, return to the General tab and click **Save Changes**.

Modifying a User Table Entry

To modify an entry SNMPv3 User Table, perform the following procedure:

- From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

- Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

- In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure**.

The SNMPv3 User Table tab is shown in Figure 70 on page 208.

- Click the button next to the SNMPv3 user that you want to change and then click **Modify**.

The Modify SNMPv3 User page is shown in Figure 72.

Engine ID	: 80:00:00:cf:03:00:30:84:fd:57:da
User Name	: debashis
Authentication Protocol	: MD5
Authentication Password	:
Confirm Authentication Password	:
Privacy Protocol	: DES
Privacy Password	:
Confirm Privacy Password	:
Storage Type	: NonVolatile
Row Status	: Active

Apply Cancel

Figure 72. Modify SNMPv3 User Page

5. In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

Select one of the following:

MD5

This value represents the MD5 authentication protocol. With this selection, users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.

SHA

This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

None

This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

Note

You may want to assign NONE to a super user.

6. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.
7. In the Confirm Authentication Password field, re-enter the authentication password.

Note

If you have the nonencrypted version of the AT-S60 software, then the Privacy Protocol field is read-only.

Note

You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

8. In the Privacy Protocol field, enter one of the following options:

DES

Select this value to make the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

None

Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

9. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.
10. In the Confirm Privacy Password field, re-enter the privacy password.
11. In the Storage Type field, enter one of the following storage options for this User Table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 User Table. After making changes to an SNMPv3 User Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 User Table. After making changes to an SNMPv3 User Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

12. Click **Apply** to update the SNMPv3 User Table.
13. To save your changes, return to the General tab and click **Save Changes**.

Configuring the SNMPv3 View Table

You can create, delete, and modify an SNMPv3 View Table entry. See the following procedures:

- ❑ "Creating a View Table Entry" on page 214
- ❑ "Deleting a View Table Entry" on page 217
- ❑ "Modifying a View Table Entry" on page 218

For reference information about the SNMPv3 View Table, see Chapter 18, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a View Table Entry

To create an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.
The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.
2. Select the **SNMP** tab.
The SNMP tab is shown in Figure 69 on page 205.
3. In the SNMPv3 section, click the button next to **Configure View Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 73.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Help Logout

General **SNMP** IGMP System Utilities Server-based Authentication Event Log

SNMPv3 View Table

Total Entries: 6. Page 1 of 2

	View Name	SubTree OID	SubTree Mask	View Type	Storage Type	Row Status
<input checked="" type="radio"/>	mgmt	1.3.6.1.2		Excluded	NonVolatile	Active
<input type="radio"/>	private	1.3.6.1.4	ff.ff	Included	Volatile	Active
<input type="radio"/>	internet	1.3.6.1		Included	NonVolatile	Active
<input type="radio"/>	directory	1.3.6.1.1		Included	NonVolatile	Active
<input type="radio"/>	experimental	1.3.6.1.3		Excluded	NonVolatile	Active

Refresh Add Remove Modify Next Back

Figure 73. SNMPv3 View Table Tab (Configuration)

- Click **Add**.

The Add New SNMPv3 View page is shown in Figure 74.

Add New SNMPv3 View

View Name : private

Subtree OID : private

Subtree Mask : ff.ff

View Type : Included ▼

Storage Type : Volatile ▼

Row Status : Active

Apply Cancel

Figure 74. Add New SNMPv3 View Page

- In the View Name field, enter a descriptive name for this view.

Assign a name that reflects the subtree OID, for example, "internet." Enter a unique name of up to 32 alphanumeric characters.

Note

The “defaultViewAll” value is the default entry for the SNMPv1 and SNMPv2c configuration. You cannot use the default value for an SNMPv3 View Table entry.

6. In the Subtree OID field, enter a subtree that this view will or will not be permitted to display.

You can enter either a numeric value in hex format or the equivalent text name. For example, the OID hex format for TCP/IP is:

1.3.6.1.2.1.6

The text format is for TCP/IP is:

tcp

7. In the Subtree Mask field, enter a subtree mask in hexadecimal format.

This is an optional parameter that is used to further refine the value of the Subtree OID parameter.

The Subtree OID parameter defines a MIB View and the Subtree Mask parameter further restricts a user’s view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB ifEntry.0.3, it has the following value:

1.3.6.1.2.1.2.2.1.0.3

To restrict the user’s view to the third row (all columns) of the MIB ifEntry.0.3, enter the following value for the Subtree Mask parameter

ff:bf

8. In the View Type field, enter one of the following view types:

Included

Enter this value to permit the user to see the subtree specified above.

Excluded

Enter this value to not permit the user to see the subtree specified above.

9. In the Storage Type field, enter a storage type for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the View Table. After making changes to a View Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the View Table. After making changes to a View Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 View Table.
11. To save your changes, return to the General tab and click **Save Changes**.

Deleting a View Table Entry

To delete an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.
The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.
2. Select the **SNMP** tab.
The SNMP tab is shown in Figure 69 on page 205.
3. In the SNMPv3 section, click the button next to **Configure View Table** and then click **Configure**.
The SNMPv3 View Table tab is shown in Figure 73 on page 215.
4. Click the button next to the View Table entry that you want to delete and then click **Remove**.
A warning message is displayed.
5. Click **OK**.
6. To save your changes, return to the General tab and click **Save Changes**.

Modifying a View Table Entry

To modify an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to Configure View Table and then click **Configure** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 73 on page 215.

4. Click the button next to the SNMPv3 View Table entry that you want to change and then click **Modify**.

The Modify SNMPv3 View page is shown in Figure 75.

Figure 75. Modify SNMPv3 View Page

5. In the Subtree Mask field, enter a subtree mask in hexadecimal format.

This is an optional parameter that is used to further refine the value of the Subtree OID parameter.

The Subtree OID parameter defines a MIB View and the Subtree Mask parameter further restricts a user's view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB ifEntry.0.3, it has the following value:

1.3.6.1.2.1.2.2.1.0.3

To restrict the user's view to the third row (all columns) of the MIB ifEntry.0.3, enter the following value for the Subtree Mask parameter

ff:bf

6. In the View Type field, enter one of the following view types:

Included

Enter this value to permit the View Name to see the subtree specified above.

Excluded

Enter this value to not permit the View Name to see the subtree specified above.

7. In the Storage Type field, enter a storage type for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the View Table. After making changes to a View Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

8. Click **Apply**.
9. To save your changes, return to the General tab and click **Save Changes**.

Configuring the SNMPv3 Access Table

You can create, delete, and modify an SNMPv3 Access Table entry. See the following procedures:

- ❑ "Creating an Access Table" on page 220
- ❑ "Deleting an Access Table Entry" on page 224
- ❑ "Modifying an Access Table Entry" on page 224

For information about the SNMPv3 Access Table, see Chapter 18, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating an Access Table

To create an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.
2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.
3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 76.

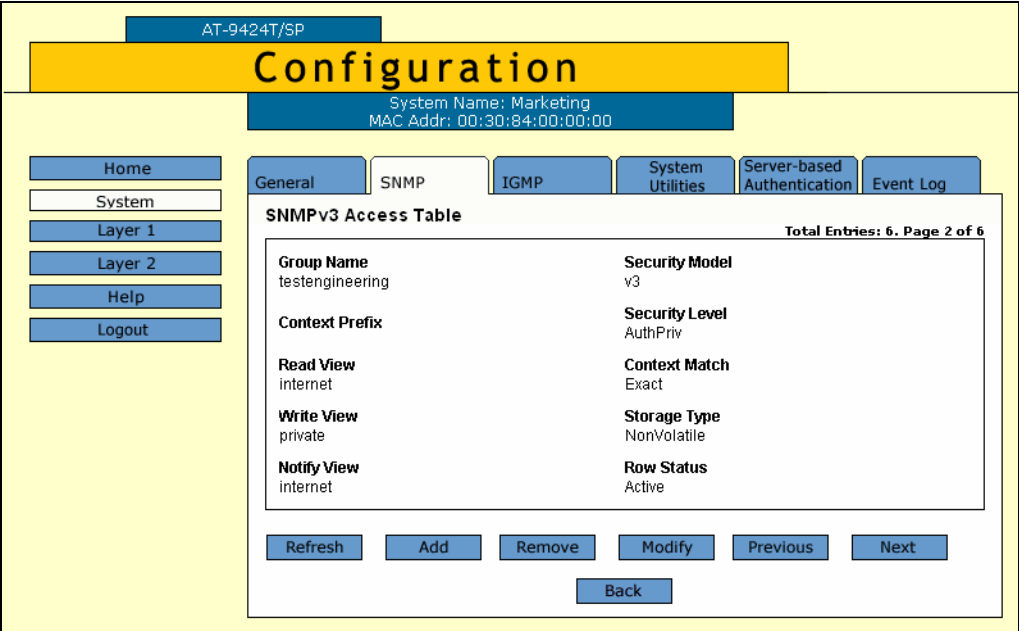


Figure 76. SNMPv3 Access Table Tab (Configuration)

4. To create an SNMPv3 Access Table entry, click **Add**.

The Add New SNMPv3 Access page is shown in Figure 77.

Add New SNMPv3 Access

Group Name	:	swengineering
Context Prefix	:	
Read View	:	internet
Write View	:	internet
Notify View	:	internet
Security Model	:	v3 ▼
Security Level	:	Privacy ▼
Context Match	:	Exact
Storage Type	:	NonVolatile ▼
Row Status	:	Active

Figure 77. Add New SNMPv3 Access Page

5. In the Group Name field, enter a descriptive name of the group.

The Group Name can consist of up to 32 alphanumeric characters.

You are not required to enter a unique value here because the SNMPv3 Access Table entry is indexed with the Group Name, Security Model, and Security Level parameter values. However, a unique group name makes it easier for you to tell the groups apart.

There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

- ☐ defaultV1GroupReadOnly
- ☐ defaultV1GroupReadWrite
- ☐ defaultV2cGroupReadOnly
- ☐ defaultV2cGroupReadWrite

Note

The Context Prefix field is a read only field. The Context Prefix field is always set to null.

6. In the Read View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

7. In the Write View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

8. In the Notify View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

9. In the Security Model field, enter an SNMP protocol.

Select one of the following SNMP protocols as the Security Model for this Group Name.

v1

Select this value to associate the Group Name with the SNMPv1 protocol.

v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

v3

Select this value to associate the Group Name with the SNMPv3 protocol.

10. In the Security Level field, enter a security level.

Select one of the following security levels:

No Authentication/Privacy

This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to

authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This option provides the least security.

Note

If you have selected SNMPv1 or SNMPv2c, N-NoAuthNoPriv is the only security level you can select.

Authentication

This option permits an authentication protocol, but not a privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy

This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Note

The Context Match field is a read only field. The Context Match field is always set to Exact.

11. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Access Table entry will take effect immediately.

12. Click **Apply**.

13. To save your changes, return to the General tab and click **Save Changes**.

Deleting an Access Table Entry

To delete an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 76 on page 221.

4. Click **Next** or **Previous** to display the Access Table entry that you want to delete.

5. Click **Remove**.

A warning message is displayed. Click OK to remove the Access Table entry.

6. To save your changes, return to the General tab and click **Save Changes**.

Modifying an Access Table Entry

To modify an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 76 on page 221.

4. Click **Next** or **Previous** to display the Access Table entry that you want to change.

5. Click **Modify**.

The Modify SNMPv3 Access page is shown in Figure 78.

Group Name	: testengineering
Context Prefix	:
Read View	: internet
Write View	: private
Notify View	: internet
Security Model	: v3
Security Level	: AuthPriv
Context Match	: Exact
Storage Type	: NonVolatile
Row Status	: Active

Apply Cancel

Figure 78. Modify SNMPv3 Access Page

Note

The Context Prefix field is a read-only field. The Context Prefix field is always set to null.

6. In the Read View Name field, enter a value that you configured with the View Name parameter in the View Table.

This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

7. In the Write View Name field, enter a value that you configured with the View Name parameter in the View Table.

This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

8. In the Notify View Name field, enter a value that you configured with the View Name parameter in the View Table.

This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

Note

The Context Match field is a read only field. The Context Match field is always set to Exact.

9. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the Access Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 Access Table.
11. To save your changes, return to the General tab and click **Save Changes**.

Configuring the SNMPv3 SecurityToGroup Table

You can create, delete, and modify an SNMPv3 SecurityToGroup Table entry. See the following procedures:

- ☐ "Creating a SecurityToGroup Table Entry" on page 227
- ☐ "Deleting a SecurityToGroup Table Entry" on page 230
- ☐ "Modifying a SecurityToGroup Table Entry" on page 230

For reference information about the SNMPv3 SecuritytoGroup Table, see Chapter 18, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a SecurityToGroup Table Entry

To create an entry in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 79.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Help Logout

General **SNMP** IGMP System Utilities Server-based Authentication Event Log

SNMPv3 SecurityToGroup Table

Total Entries: 19. Page 5 of 5

	Security Model	Security Name	Group Name	Storage Type	Row Status
<input checked="" type="radio"/>	v3	jenny	swengineering	NonVolatile	Active
<input type="radio"/>	v3	chitra	testengineering	NonVolatile	Active
<input type="radio"/>	v3	debashis	swengineering	NonVolatile	Active

Refresh Add Remove Modify Previous Back

Figure 79. SNMPv3 SecurityToGroup Table Tab (Configuration)

- To create an SNMPv3 SecurityToGroup Table entry, click **Add**.

The Add New SNMPv3 SecurityToGroup page is shown in Figure 80.

Add New SNMPv3 SecurityToGroup

Security Model : v3

Security Name : chitra

Group Name : testengineering

Storage Type : NonVolatile

Row Status : Active

Apply Cancel

Figure 80. Add New SNMPv3 SecurityToGroup Page

- In the Security Model field, select the SNMP protocol that was configured for this User Name.

Choose from the following:

v1

Select this value to associate the Group Name with the SNMPv1 protocol.

v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

v3

Select this value to associate the Group Name with the SNMPv3 protocol.

6. In the Security Name field, enter the User Name that you want to associate with a group.

Enter a User Name that you configured in "Creating a User Table Entry" on page 207.

7. In the Group Name field, enter a Group Name that you configured in the Access Table.

See "Creating an Access Table" on page 220.

There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

- ☐ defaultV1GroupReadOnly
- ☐ defaultV1GroupReadWrite
- ☐ defaultV2cGroupReadOnly
- ☐ defaultV2cGroupReadWrite

8. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

9. Click **Apply**.
10. To save your changes, return to the General tab and click **Save Changes**.

Deleting a SecurityToGroup Table Entry

To delete an entry SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.
The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.
2. Select the **SNMP** tab.
The SNMP tab is shown in Figure 69 on page 205.
3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table**, and then click **Configure** at the bottom of the tab.
The SNMPv3 SecurityToGroup Table tab is shown in Figure 79 on page 228.
4. Click the button next to the SecurityToGroup Table entry that you want to delete and then click **Remove**.
A warning message is displayed.
5. Click **OK**.
6. To save your changes, return to the General tab and click **Save Changes**.

Modifying a SecurityToGroup Table Entry

To modify an entry SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.
The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.
2. Select the **SNMP** tab.
The SNMP tab is shown in Figure 69 on page 205.
3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table** and then click **Configure** at the bottom of the tab.
The SNMPv3 SecurityToGroup Table tab is shown in Figure 79 on page 228.

- Click the button next to the SecurityToGroup Table entry that you want to change, and then click **Modify**.

The Modify SNMPv3 SecurityToGroup page is shown in Figure 81.

Figure 81. Modify SNMPv3 SecurityToGroup Page

- In the Group Name field, enter a Group Name that you configured in the SNMPv3 Access Table.

See "Creating an Access Table" on page 220.

There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

- ☐ defaultV1GroupReadOnly
- ☐ defaultV1GroupReadWrite
- ☐ defaultV2cGroupReadOnly
- ☐ defaultV2cGroupReadWrite

- In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

7. Click **Apply** to update the SNMPv3 SecurityToGroup Table.
8. To save your changes, return to the General tab and click **Save Changes**.

Configuring the SNMPv3 Notify Table

You can create, delete, and modify an SNMPv3 Notify Table entry. See the following procedures:

- ☐ "Creating a Notify Table Entry" on page 233
- ☐ "Deleting a Notify Table Entry" on page 235
- ☐ "Modifying a Notify Table Entry" on page 236

For reference information about the SNMPv3 Notify Table, see Chapter 18, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Notify Table Entry

To create an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.
2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.
3. In the SNMPv3 section, click the button next to **Configure Notify Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 82.

SNMPv3 Notify Table					Total Entries: 16. Page 4 of 4
	Notify Name	Notify Tag	Notify Type	Storage Type	Row Status
<input checked="" type="radio"/>	swenginformat	swenginformatag	Inform	NonVolatile	Active
<input type="radio"/>	swengtrap	swengtag	Trap	NonVolatile	Active
<input type="radio"/>	testenginformat	testenginformatag	Inform	NonVolatile	Active
<input type="radio"/>	testengtrap	testengtag	Trap	NonVolatile	Active

Figure 82. SNMPv3 Notify Table Tab (Configuration)

4. Click **Add**.

The Add New SNMPv3 Notify page is shown in Figure 83.

Figure 83. Add New SNMPv3 Notify Page

5. In the Notify Name field, enter the name associated with this trap message.

Enter a descriptive name of up to 32 alphanumeric characters. For example, you might want to define a trap message for hardware engineering and enter a value of "hardwareengineeringtrap" for the Notify Name.

6. In the Notify Tag field, enter a description name of the Notify Tag.

Enter a name of up to 32 alphanumeric characters.

7. In the Notify Type field, enter one of the following message types:

Trap

Indicates this notify table is used to send traps. With this message type, the switch does not expect a response from the host.

Inform

Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

8. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Notify Table. After making changes to a Notify Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Notify Table. After making changes to a Notify Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Notify Table.
10. To save your changes, return to the General tab and click **Save Changes**.

Deleting a Notify Table Entry

To delete an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Notify Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 82 on page 234.

- Click the button next to the Notify Table entry that you want to delete, and then click **Remove**.

A warning message is displayed.

- Click **OK**.
- To save your changes, return to the General tab and click **Save Changes**.

Modifying a Notify Table Entry

To modify an entry in the SNMPv3 Notify Table, perform the following procedure:

- From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

- Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

- In the SNMPv3 section, click the button next to Configure Notify Table, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 82 on page 234.

- Click the button next to the table entry that you want to change and then click **Modify**.

The Modify SNMPv3 Notify page is shown in Figure 84.

Figure 84. Modify SNMPv3 Notify Page

- In the Notify Tag field, enter a description name of the Notify Tag. Enter a name of up to 32 alphanumeric characters.
- In the Notify Type field, enter one of the following message types:

Trap

Indicates this notify table is used to send traps. With this message type, the switch does not expect a response from the host.

Inform

Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

7. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Notify Table. After making changes to an Notify Table entry with a Volatile storage type, **Save Changes** does not appear on the Configuration Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Notify Table. After making changes to an Notify Table entry with a NonVolatile storage type, **Save Changes** appears on the Configuration Tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

8. Click **Apply** to update the SNMPv3 Notify Table.
9. To save your changes, return to the General tab and click **Save Changes**.

Configuring the SNMPv3 Target Address Table

You can create, delete, and modify an SNMPv3 Target Address Table entry. See the following procedures:

- ❑ "Creating a Target Address Table Entry" on page 238
- ❑ "Deleting a Target Address Table Entry" on page 241
- ❑ "Modifying Target Address Table Entry" on page 242

For reference information about the SNMPv3 Target Address Table, see Chapter 18, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Target Address Table Entry

To create an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.
The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.
2. Select the **SNMP** tab.
The SNMP tab is shown in Figure 69 on page 205.
3. In the SNMPv3 section, click the button next to **Configure Target Address Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 85.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home

System

Layer 1

Layer 2

Help

Logout

General
SNMP
IGMP
System Utilities
Server-based Authentication
Event Log

SNMPv3 Target Address Table

Total Entries: 20. Page 20 of 20

Target Address snmpv3host100	Timeout 2500
Parameters snmpv3manager100	Retries 7
IP Address 194.1.1.1	UDP Port Number 162
Storage Type NonVolatile	Row Status Active
Tag List hwengtag swengtag testengtag	

Refresh
Add
Remove
Modify
Previous

Back

Figure 85. SNMPv3 Target Address Table Tab (Configuration)

4. Click **Add**.

The Add New SNMPv3 Target Address page is shown in Figure 86.

Add New SNMPv3 Target Address

Target Address Name :

IP Address :

UDP Port Number :

Timeout :

Retries :

Tag List :

Target Parameters :

Storage Type : Volatile ▼

Row Status : Active

Apply
Cancel

Figure 86. Add New SNMPv3 Target Address Page

5. In the Target Address Name field, enter the name of the SNMP manager, or host, that manages the SNMP activity on your switch.

You can enter a name of up to 32 alphanumeric characters.

6. In the IP Address field, enter the IP address of the host.

Use the following format for an IP address:
XXX.XXX.XXX.XXX

7. In the UDP Port Number field, enter a UDP port number.

You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

8. In the Timeout field, enter a timeout value in milliseconds.

When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

9. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

10. In the Tag List field, enter a list of tags that you configured in a SNMPv3 Notify Table with the Notify Tag parameter.

See "Creating a Notify Table Entry" on page 233. Enter a Tag List of up to 256 alphanumeric characters. Use a space to separate entries, for example:

hwengtag swengtag testengtag

11. In the Target Parameters field, enter a Target Parameters name.

This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the SNMPv3 Target Parameters Table.

12. In the Storage Type field, enter one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Address Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 Target Address Table.
14. To save your changes, return to the General tab and click **Save Changes**.

Deleting a Target Address Table Entry

To delete an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 85 on page 239.

4. Click **Next** or **Previous** to display the SNMPv3 Target Address Table entry that you want to delete.
5. Click **Remove**.

A warning message is displayed.

6. Click **OK**.

7. To save your changes, return to the General tab and click **Save Changes**.

Modifying Target Address Table Entry

To modify an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 85 on page 239.

4. Click **Next** or **Previous** to display the Target Address Table entry that you want to change.

5. Click **Modify**.

The Modify SNMPv3 Target Address page is shown Figure 87.

Target Address Name	: snmpv3host50
IP Address	: 192.1.1.1
UDP Port Number	: 162
Timeout	: 1500
Retries	: 7
Tag List	: swengtag hwengtag
Target Parameters	: snmpv3manager50
Storage Type	: Volatile
Row Status	: Active

Apply Cancel

Figure 87. Modify SNMPv3 Target Address Page

6. In the IP Address field, enter the IP address of the host.

Use the following format for an IP address:

XXX.XXX.XXX.XXX

7. In the UDP Port Number field, enter a UDP port number.

You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

8. In the Timeout field, enter a timeout value in milliseconds.

When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

9. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

10. In the Tag List field, enter a list of tags that you configured with the Notify Tag parameter in a Notify Table entry.

See "Creating a Notify Table Entry" on page 233. Enter a Tag List of up to 256-alphanumeric characters. Use a space to separate entries, for example:

hwengtag swengtag testengtag

11. In the Target Parameters field, enter a Target Parameters name.

This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the Target Parameters Table.

12. In the Storage Type field, enter one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Address Table. After making changes to an Target Address Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

13. Click **Apply** to update the SNMPv3 Target Address Table.
14. To save your changes, return to the General tab and click **Save Changes**.

Configuring the SNMPv3 Target Parameters Table

You can create, delete, and modify an SNMPv3 Target Parameters Table entry. See the following procedures:

- ❑ "Creating a Target Address Table Entry" on page 238
- ❑ "Deleting a Target Address Table Entry" on page 241
- ❑ "Modifying Target Address Table Entry" on page 242

For reference information about the SNMPv3 Target Parameters Table, see Chapter 18, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Target Parameters Table Entry

To create an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 88.

The screenshot shows the 'Configuration' page for 'AT-9424T/SP'. The 'SNMP' tab is selected. Below the tab, the 'SNMPv3 Target Parameters Table' is displayed with 11 total entries. The table has columns for Params Name, Message Processing Model, Security Model, Security Name, Security Level, Storage Type, and Row Status. Three entries are visible: snmpv3manager100, snmpv3manager150, and snmpv3manager50. Below the table are buttons for Refresh, Add, Remove, Modify, Previous, and Back.

	Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
<input checked="" type="radio"/>	snmpv3manager100	v3	v3	chitra	AuthPriv	NonVolatile	Active
<input type="radio"/>	snmpv3manager150	v3	v3	luke	AuthPriv	Volatile	Active
<input type="radio"/>	snmpv3manager50	v3	v3	debashi	AuthPriv	Volatile	Active

Figure 88. SNMPv3 Target Parameters Table Tab (Configuration)

4. Click **Add**.

The Add New SNMPv3 Target Parameter page is shown in Figure 89.

Add New SNMPv3 Target Parameter

Target Parameters Name : snmpv3manager50

Message Processing Model : v3

Security Model : v3

Security Name : debashi

Security Level : Privacy

Storage Type : Volatile

Row Status : Active

Apply Cancel

Figure 89. Add New SNMPv3 Target Parameters Page

5. In the Target Parameters Name field, enter a name of the SNMP manager or host.

Enter a value of up to 32 alphanumeric characters.

Note

Enter a value for the Message Processing Model parameter only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the Message Processing Model is automatically assigned to SNMPv3.

6. In the Message Processing Model field, enter a Security Model that is used to process messages.

Select one of the following SNMP protocols:

v1

Select this value to process messages with the SNMPv1 protocol.

v2c

Select this value to process messages with the SNMPv2c protocol.

v3

Select this value to process messages with the SNMPv3 protocol.

7. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

v1

Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

v2c

Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

v3

Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

8. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

See "Creating a User Table Entry" on page 207.

9. In the Security Level field, select one of the following Security Levels:

Note

The value you configure for the Security Level must match the value configured for the User Name in the User Table Menu. See "Creating a User Table Entry" on page 207.

No Authentication/Privacy

This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

Note

If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

Authentication

This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy

This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

10. In the Storage Type parameter, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to a Target Parameters Table entry with a Volatile storage type, then **Save Changes** does not appear on the Configuration Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Parameters Table. After making changes to a Target Parameters Table entry with a NonVolatile storage type, then **Save Changes** appears on the Configuration Tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Parameters Table entry takes effect immediately.

11. Click **Apply** to update the SNMPv3 Target Parameters Table.
12. To save your changes, return to the General tab and click **Save Changes**.

Deleting a Target Parameters Table Entry

To delete an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 88 on page 245.

4. Click the button next to the Target Parameters Table entry that you want to delete and then click **Remove**.

A warning message is displayed.

5. Click **OK**.

- To save your changes, return to the General tab and click **Save Changes**.

Modifying a Target Parameters Table Entry

To modify an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

- From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

- Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

- In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 88 on page 245.

- Click the button next to the Target Parameters Table entry that you want to change, and then click **Modify**.

The Modify SNMPv3 Target Parameter page is shown in Figure 90 on page 249.

Target Parameters Name	: snmpv3manager100
Message Processing Model	: v3
Security Model	: v3
Security Name	: chitra
Security Level	: Privacy
Storage Type	: NonVolatile
Row Status	: Active

Apply Cancel

Figure 90. Modify SNMPv3 Target Parameter Page

Note

Enter a value for the Message Processing Model field only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the switch automatically assigns the Message Processing Model to SNMPv3.

5. In the Message Processing Model field, enter a Security Model that is used to process messages.

Select one of the following SNMP protocols:

v1

Select this value to process messages with the SNMPv1 protocol.

v2c

Select this value to process messages with the SNMPv2c protocol.

v3

Select this value to process messages with the SNMPv3 protocol.

6. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

v1

Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

v2c

Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

v3

Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

7. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

See "Creating a User Table Entry" on page 207.

8. In the Security Level field, select one of the following Security Levels:

Note

The value you configure for the Security Level must match the value configured for the User Name in the SNMPv3 User Table Menu. See "Creating a User Table Entry" on page 207.

No Authentication/Privacy

This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

Note

If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

Authentication

This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy

This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

9. In the Storage Type parameter, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Parameters Table entry will take effect immediately.

10. Click **Apply** to update the SNMPv3 Target Parameters Table.
11. To save your changes, return to the General tab and click **Save Changes**.

Configuring the SNMPv3 Community Table

You can create, delete, and modify an SNMPv3 Community Table entry. See the following procedures:

- ❑ "Creating an SNMPv3 Community Table Entry" on page 252
- ❑ "Deleting an SNMPv3 Community Table Entry" on page 255
- ❑ "Modifying an SNMPv3 Community Table Entry" on page 255

For reference information about the SNMPv3 Community Table, see Chapter 18, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Note

Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesyn does not recommend this configuration.

Creating an SNMPv3 Community Table Entry

To create an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Community Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 91.

The screenshot shows the 'Configuration' page for 'AT-9424T/SP'. The 'System Name' is 'Marketing' and the 'MAC Addr' is '00:30:84:00:00:00'. The 'SNMP' tab is selected. The 'SNMPv3 Community Table' section shows a table with 4 entries. The table has columns: Community Index, Community Name, Security Name, Transport Tag, Storage Type, and Row Status. The entries are: California (SantaClara456, wilson, swengtag testengtag, NonVolatile, Active), alabama (birmingham123, jenny, swengtag, NonVolatile, Active), carolina (raleigh998, chitra, testengtag, NonVolatile, Active), and dakota (bismarck778, hoa, hwengtag swengtag, NonVolatile, Active). Below the table are buttons for Refresh, Add, Remove, Modify, and Back.

Community Index	Community Name	Security Name	Transport Tag	Storage Type	Row Status
California	SantaClara456	wilson	swengtag testengtag	NonVolatile	Active
alabama	birmingham123	jenny	swengtag	NonVolatile	Active
carolina	raleigh998	chitra	testengtag	NonVolatile	Active
dakota	bismarck778	hoa	hwengtag swengtag	NonVolatile	Active

Figure 91. SNMPv3 Community Table Tab (Configuration)

- Click **Add**.

The Add New SNMPv3 Community page is shown in Figure 92.

The screenshot shows the 'Add New SNMPv3 Community' page. It has fields for Community Index, Community Name, Security Name, Transport Tag, Storage Type, and Row Status. The values entered are: Community Index: 10456, Community Name: SantaClaraCA333, Security Name: murthy, Transport Tag: swengtag swenginform, Storage Type: NonVolatile (dropdown), and Row Status: Active. There are 'Apply' and 'Cancel' buttons at the bottom.

Figure 92. Add New SNMPv3 Community Page

- In the Community Index field, enter a numerical value for this Community.

This parameter is used to index the other parameters in an SNMPv3 Community Table entry. Enter a value of up to 32-alphanumeric characters.

- In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

Note

Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

7. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

This name must be unique. Enter a value of up to 32 alphanumeric characters.

Note

Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

8. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See "Creating a Target Address Table Entry" on page 238.

9. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

10. Click **Apply**.

11. To save your changes, return to the General tab and click **Save Changes**.

Deleting an SNMPv3 Community Table Entry

To delete an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Community Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 91 on page 253.

4. Click the button next to the SNMPv3 Community Table entry that you want to delete and then click **Remove**.

A warning message is displayed.

5. Click **OK**.

6. To save your changes, return to the General tab and click **Save Changes**.

Modifying an SNMPv3 Community Table Entry

To modify an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 69 on page 205.

3. In the SNMPv3 section, click the button next to **Configure Community Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 91 on page 253.

4. Click the button next to the SNMPv3 Community Table entry that you want to change and then click **Modify**.

The Modify SNMPv3 Community page is shown in Figure 93.

Community Index	: alabama
Community Name	: <input type="text" value="birmingham123"/>
Security Name	: <input type="text" value="jenny"/>
Transport Tag	: <input type="text" value="swengtag"/>
Storage Type	: <input type="text" value="NonVolatile"/>
Row Status	: Active

Figure 93. Modify SNMPv3 Community Page

5. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

Note

Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

6. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

This name must be unique. Enter a value of up to 32 alphanumeric characters.

Note

Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

7. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See "Creating a Target Address Table Entry" on page 238.

8. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, **Save Changes** does not appear on the General tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, **Save Changes** appears on the General tab, allowing you to save your changes. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Community Table.
10. To save your changes, return to the General tab and click **Save Changes**.

Displaying SNMPv3 Tables

This section contains procedures to display the SNMPv3 Tables. The following procedures are provided:

- ❑ "Displaying User Table Entries" on page 259
- ❑ "Displaying View Table Entries" on page 261
- ❑ "Displaying Access Table Entries" on page 262
- ❑ "Displaying SecurityToGroup Table Entries" on page 263
- ❑ "Displaying Notify Table Entries" on page 264
- ❑ "Displaying Target Address Table Entries" on page 265
- ❑ "Displaying Target Parameters Table Entries" on page 266
- ❑ "Displaying SNMPv3 Community Table Entries" on page 267

Displaying User Table Entries

To display entries in the SNMPv3 User Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 94.

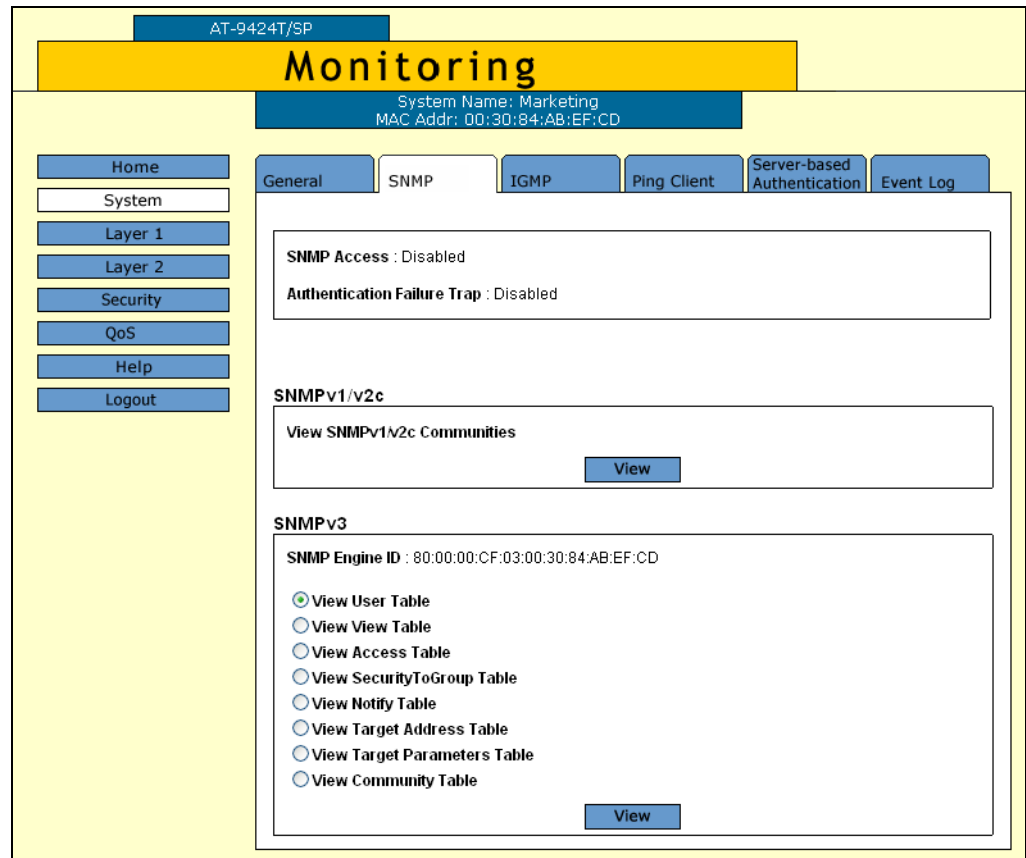


Figure 94. SNMP Tab (Monitoring)

3. In the SNMPv3 section, click the button next to View User Table and then click **View** at the bottom of the tab.

The SNMPv3 User Table tab is shown in Figure 95.

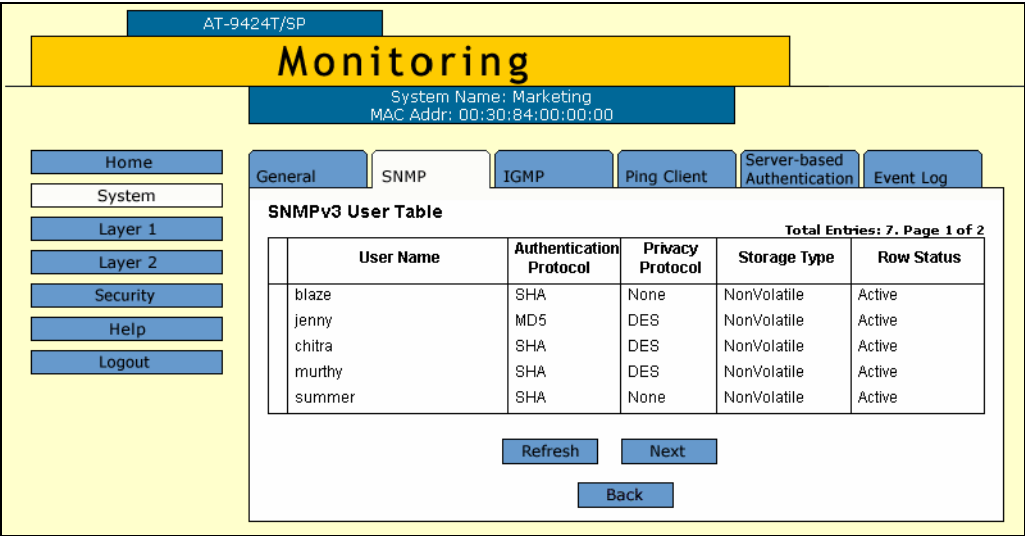


Figure 95. SNMPv3 User Table Tab (Monitoring)

Displaying View Table Entries

To display entries in the SNMPv3 View Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 94 on page 259.

3. In the SNMPv3 section, click the button next to **View View Table** and then click **View** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 96.

The screenshot shows the AT-9424T/SP Monitoring page. The top navigation bar includes 'Home', 'System', 'Layer 1', 'Layer 2', 'Security', 'Help', and 'Logout'. The main content area has tabs for 'General', 'SNMP', 'IGMP', 'Ping Client', 'Server-based Authentication', and 'Event Log'. The 'SNMP' tab is selected, and the 'SNMPv3 View Table' is displayed. The table has columns for View Name, SubTree OID, SubTree Mask, View Type, Storage Type, and Row Status. The table contains five rows of data. Below the table are buttons for 'Refresh', 'Next', and 'Back'.

View Name	SubTree OID	SubTree Mask	View Type	Storage Type	Row Status
mgmt	1.3.6.1.2		Excluded	NonVolatile	Active
private	1.3.6.1.4	ff.ff	Included	Volatile	Active
internet	1.3.6.1		Included	NonVolatile	Active
directory	1.3.6.1.1		Included	NonVolatile	Active
experimental	1.3.6.1.3	ff.ff.ff	Excluded	NonVolatile	Active

Figure 96. SNMPv3 View Table Tab (Monitoring)

Displaying Access Table Entries

To display entries in the SNMPv3 Access Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 94 on page 259.

3. In the SNMPv3 section, click the button next to **View Access Table** and then click **View** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 97.

The screenshot shows a web interface for a monitoring system. At the top, there's a header bar with 'AT-9424T/SP' and a large yellow 'Monitoring' title. Below the title, system information is displayed: 'System Name: Marketing' and 'MAC Addr: 00:30:84:00:00:00'. A navigation menu on the left includes 'Home', 'System', 'Layer 1', 'Layer 2', 'Security', 'Help', and 'Logout'. The main content area has several tabs: 'General', 'SNMP', 'IGMP', 'Ping Client', 'Server-based Authentication', and 'Event Log'. The 'SNMP' tab is active, showing the 'SNMPv3 Access Table'. The table has two columns: 'Group Name' and 'Security Model'. The first row shows 'techpubs' and 'v3'. Below the table, there are buttons for 'Refresh', 'Next', and 'Back'. The text 'Total Entries: 5, Page 1 of 5' is displayed in the top right corner of the table area.

Group Name	Security Model
techpubs	v3

Context Prefix: internet1
Read View: internet1
Write View: internet1
Notify View: internet1

Security Level: AuthPriv
Context Match: Exact
Storage Type: NonVolatile
Row Status: Active

Buttons: Refresh, Next, Back

Total Entries: 5, Page 1 of 5

Figure 97. SNMPv3 Access Table Tab (Monitoring)

Displaying SecurityToGroup Table Entries

To display entries in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 94 on page 259.

3. In the SNMPv3 section, click the button next to the **View SecurityToGroup Table** and then click **View** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 98.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home

System

Layer 1

Layer 2

Security

Help

Logout

General

SNMP

IGMP

Ping Client

Server-based Authentication

Event Log

SNMPv3 SecurityToGroup Table

Total Entries: 5. Page 1 of 2

	Security Model	Security Name	Group Name	Storage Type	Row Status
	v3	hoa	swengineering	NonVolatile	Active
	v3	luke	testengineering	NonVolatile	Active
	v3	jenny	swengineering	NonVolatile	Active
	v3	chitra	testengineering	NonVolatile	Active
	v3	debashis	swengineering	NonVolatile	Active

Refresh

Next

Back

Figure 98. SNMPv3 SecurityToGroup Table Tab (Monitoring)

Displaying
Notify Table
Entries

To display entries in the SNMPv3 Notify Table, perform the following procedure:

- 1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

- 2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 94 on page 259.

- 3. In the SNMPv3 section, click the button next to **View Notify Table** and then click **View** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 99.

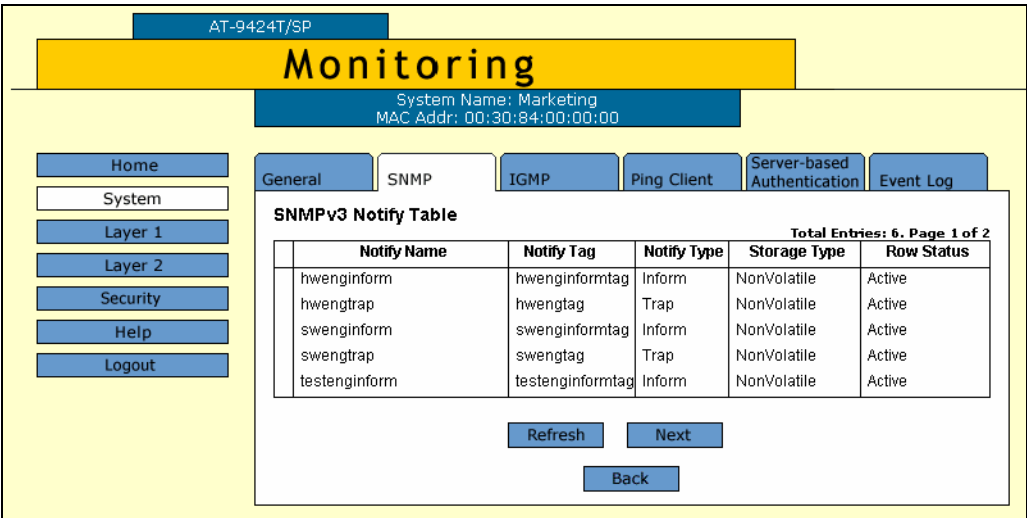


Figure 99. SNMPv3 Notify Table Tab (Monitoring)

Displaying Target Address Table Entries

To display entries in the SNMPv3 Target Address Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** Tab.

The SNMP tab is shown in Figure 94 on page 259.

3. In the SNMPv3 section, lick the button next to **View Target Address Table** and then click **View** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 100.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security Help Logout

General **SNMP** IGMP Ping Client Server-based Authentication Event Log

SNMPv3 Target Address Table

Total Entries: 2. Page 1 of 2

Target Address snmpv3host1	Timeout 1500
Parameters snmpv3manager1	Retries 2
IP Address 187.1.1.1	UDP Port Number 162
Storage Type NonVolatile	Row Status Active
Tag List testengtag swengtag	

Refresh Next Back

Figure 100. SNMPv3 Target Address Table Tab (Monitoring)

Displaying Target Parameters Table Entries

To display entries in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 94 on page 259.

3. In the SNMPv3 section, click the button next to the **View Target Parameters Table** and then click **View** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 100.

The screenshot shows a web interface for a monitoring system. At the top, there's a header with 'AT-9424T/SP' and a large yellow 'Monitoring' banner. Below the banner, system information is displayed: 'System Name: Marketing' and 'MAC Addr: 00:30:84:00:00:00'. A navigation menu on the left includes 'Home', 'System', 'Layer 1', 'Layer 2', 'Security', 'Help', and 'Logout'. The main content area has several tabs: 'General', 'SNMP', 'IGMP', 'Ping Client', 'Server-based Authentication', and 'Event Log'. The 'SNMP' tab is selected, showing the 'SNMPv3 Target Parameters Table'. The table has 7 columns: 'Params Name', 'Message Processing Model', 'Security Model', 'Security Name', 'Security Level', 'Storage Type', and 'Row Status'. It contains 6 entries, all with 'v3' for the message processing and security models, and 'Active' for the row status. Below the table are 'Refresh', 'Next', and 'Back' buttons.

Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
manager50	v3	v3	jenny	AuthPriv	NonVolatile	Active
snmpmanager65	v3	v3	murthy	AuthPriv	NonVolatile	Active
snmpmanager75	v3	v3	teresa	AuthPriv	NonVolatile	Active
snmpv3manager120	v3	v3	hoa	AuthNoPriv	NonVolatile	Active
snmpv3manager220	v3	v3	luke	AuthNoPriv	NonVolatile	Active

Figure 101. SNMPv3 Target Parameters Table Tab (Monitoring)

Displaying SNMPv3 Community Table Entries

To display entries in the SNMPv3 Community Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 94 on page 259.

3. In the SNMPv3 section, click the button next to **View Community Table** and then click **View** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 102.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security Help Logout

General **SNMP** IGMP Ping Client Server-based Authentication Event Log

SNMPv3 Community Table

Total Entries: 5, Page 1 of 2

Community Index	Community Name	Security Name	Transport Tag	Storage Type	Row Status
10456	SantaClara5	tomas	testengtag testengininform	NonVolatile	Active
10555	SanJose78	ross	testengtag testengininform	NonVolatile	Active
10650	Sunnyvale45	nelwid	swengtag swengininform	NonVolatile	Active
10675	Fremont7	loan	hwengtag hwengininform	NonVolatile	Active
10725	Campbell98	frankk	testengtag testengininform	NonVolatile	Active

Refresh Next Back

Figure 102. SNMPv3 Community Table Tab (Monitoring)

Section III

VLANs

The chapters in this section explain how to set up security on an AT-9400 Series switch. The chapters include:

- ❑ Chapter 17, "Virtual LANs" on page 271
- ❑ Chapter 18, "GARP VLAN Registration Protocol (GVRP)" on page 285

Chapter 17

Virtual LANs

This chapter explains how to create, modify, and delete port-based and tagged VLANs. This chapter also explains how to select a multiple VLAN mode.

This chapter contains the following sections:

- ☐ "Creating a New Port-Based or Tagged VLAN" on page 272
- ☐ "Modifying a VLAN" on page 276
- ☐ "Deleting a VLAN" on page 278
- ☐ "Selecting a VLAN Mode" on page 279
- ☐ "Displaying VLANs" on page 281
- ☐ "Specifying a Management VLAN" on page 283

Note

For background information on port-based and tagged VLANs, as well as management VLANs, refer to Chapter 19, "Port-based and Tagged VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*. For more information about the multiple VLAN modes, refer to Chapter 20, "Multiple VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a New Port-Based or Tagged VLAN

To create a new port-based or tagged VLAN, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 103.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

MAC Address **VLAN** GVRP Spanning Tree Enhanced Stacking

VLAN Mode
☒ User Configured ☐ Multiple ☐ Multiple 802.1Q
Mgmt. VLAN ID

Uplink Port

Apply

Total VLANs: 4. Page 1 of 1

	VLAN ID	(Client) Name	Uplink Port	Type	Protocol	Tagged(T)/Untagged(U) Ports
<input checked="" type="radio"/>	1	Default_VLAN	NA	Port Based	None	U: 1-2,17,23-24
<input type="radio"/>	3	Sales	NA	Port Based	None	U: 5-10,15-16 T: 17
<input type="radio"/>	54	Production	NA	Port Based	None	U: 19-22 T: 17
<input type="radio"/>	24	Engineering	NA	Port Based	None	U: 3-4,11-14,18 T: 17

Refresh Add Modify Remove

Figure 103. VLAN Tab (Configuration)

Note

The Modify and Remove buttons are not shown in the tab if the only VLAN on the switch is the Default_VLAN.

The VLAN Mode and Uplink Port options are explained in "Selecting a VLAN Mode" on page 279. The Mgmt. VLAN ID option is explained in "Specifying a Management VLAN" on page 283.

The tab displays an existing VLANs on the switch.

4. To add a new VLAN, click **Add**.

The Add New VLAN page is shown in Figure 104.

Figure 104. Add New VLAN Page

5. Adjust the following parameters as necessary.

VID

Enter a VID value for the new VLAN. The range of the VID value is 2 to 4096. The default is the next available VID number on the switch.

If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, you should assign the Sales VLAN on each switch the same VID value.

Note

A VLAN must have a VID.

It is important to note that the switch is only aware of the VIDs of the VLANs that exist on the device, and not those that might already be in use in the network. For example, if you add a new AT-9400 Series switch to a network that already contains VLANs that use VIDs 2 through 24, the AT-S63 management software still uses VID 2 as the default value when you create the first VLAN on the new switch, even though that VID number is already being used by another VLAN on

the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

Name

Specify a name for the new VLAN.

The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that are part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

If the VLAN is unique in your network, then the name should be unique as well. If the VLAN is part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

Note

A VLAN must be assigned a name.

6. To select the ports for the VLAN, click on the appropriate ports in the switch image.

Clicking repeatedly on a port toggles the port through the following possible settings:



Untagged port



Tagged port



Port not a member of the VLAN

Note

When a transceiver is inserted into an uplink slot and a link is established, that slot becomes a primary uplink port and the corresponding backup port, 23R or 24R, automatically transitions to redundant uplink status. Any VLAN settings remain intact when the backup port makes the transition to a redundant uplink state.

7. Click **Apply**.

Note

Any untagged ports that you assign to the new VLAN are automatically removed from their current untagged VLAN assignment.

The new user-configured VLAN is now ready for network operations.

8. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Modifying a VLAN

This procedure explains how to add or remove ports from a VLAN. When modifying a VLAN, note the following:

- ☐ You cannot change the VID of a VLAN.
- ☐ You cannot change the name of a VLAN from a web browser management session, but you can from a local or Telnet session.
- ☐ You cannot modify VLANs when the switch is operating in one of the multiple VLAN modes.

To modify a VLAN, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 103 on page 272.

4. Click the button next to the name of the VLAN you want to modify.
5. Click **Modify**.

The Modify VLAN page for the VLAN is displayed.

6. To add or remove ports from the VLAN, click on the appropriate ports in the switch image.

Clicking repeatedly on a port toggles the port through the following possible settings:



Untagged port



Tagged port



Port not a member of the VLAN

7. Click **Apply**.

Note

Untagged ports that are added to a VLAN are automatically removed from their current untagged VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

Removing an untagged port from the Default_VLAN without assigning it to another VLAN leaves the port as an untagged member of no VLAN.

The modified VLAN is now ready for network operations.

8. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Deleting a VLAN

To delete a port-based or tagged VLAN from the switch, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 103 on page 272.

4. Click the button next to the name of the VLAN you want to delete. (You cannot delete the Default_VLAN.)

5. Click **Remove**.

A confirmation prompt is displayed.

6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure:

If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.

7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Selecting a VLAN Mode

The AT-S63 management software features three VLAN modes:

- ☐ Port-based and tagged VLAN Mode (default mode)
- ☐ IEEE 802.1Q-compliant Multiple VLAN Mode
- ☐ Non-IEEE 802.1Q compliant Multiple VLAN Mode

For background information on port-based and tagged VLANs, refer to Chapter 19, "Port-based and Tagged VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*. For information on the multiple VLAN modes, refer to Chapter 20, "Multiple VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*.

Note

Any port-based or tagged VLANs that you may have created are not retained when you change the VLAN mode from the user configured mode to a multiple VLAN mode and, at some point, reset the switch. The user configured VLAN information is lost and you must recreate the information if you later return the switch to the user configured VLAN mode.

To select a VLAN mode for the switch, perform the procedure below:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 103 on page 272.

4. In the VLAN Mode section, select a VLAN mode. Only one mode can be active on the switch at a time. The modes are:

User Configured - Port-based and tagged VLAN Mode

Multiple - Non-IEEE 802.1Q-compliant Multiple VLAN Mode

Multiple 802.1Q - IEEE 802.1Q-compliant Multiple VLAN Mode

5. If you select one of the multiple VLAN modes, specify an uplink port in the Uplink Port field. This port functions as the uplink port for the VLANs. The default is port 1.
6. Click **Apply**.

The new mode is automatically activated on the switch.

7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying VLANs

To display the current VLANs on a switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 105.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

MAC Address **VLAN** GVRP Spanning Tree Port Security Enhanced Stacking

VLAN Mode
User Configured
Management VLAN ID
1

Total VLANs: 4. Page 1 of 1

VLAN ID	Name	Uplink Port	Type	Protocol	Tagged(T)/Untagged(U) Ports
1	Default_VLAN	NA	Port Based	None	U: 1-2,17,23-24
3	Sales	NA	Port Based	None	U: 5-10,15-16
		NA		None	T: 17
54	Production	NA	Port Based	None	U: 19-22
		NA		None	T: 17
24	Engineering	NA	Port Based	None	U: 3-4,11-14,18
		NA		None	T: 17

Refresh

Figure 105. VLAN Tab (Monitoring)

The upper part of the tab displays the following information:

Mode

The VLAN mode. The possible settings are:

User Configured - This mode supports port-based and tagged VLANs.

Multiple 802.1Q - The IEEE 802.1Q-compliant multiple VLAN mode.

Multiple - The non-IEEE 802.1Q-compliant multiple VLAN mode.

Management VLAN ID

VLAN ID of the management VLAN.

The lower part of the tab displays a table that contains the following columns of information:

VLAN ID

The VID number assigned to the VLAN.

(Client) Name

The name of the VLAN. If the switch is operating in one of the multiple VLAN modes, the names of the VLANs start with "Client," with the exception of the VLAN containing the uplink port, which starts with "Uplink."

Uplink Port

This column is applicable only when the switch is operating in one of the two multiple VLAN modes. The column lists the port that is functioning as the uplink port for all the other ports on the switch.

VLAN Type

The VLAN type. The possible settings are:

Port Based - The VLAN is a port-based or tagged VLAN.

GARP - The VLAN was automatically created by GARP.

Protocol

The protocol associated with this VLAN. The possible settings are:

Blank - The VLAN is a port-based or tagged VLAN.

GARP - The VLAN is a dynamic GVRP VLAN or the port is a dynamic GVRP port of a static VLAN.

Tagged(T)/Untagged(U) Port

Lists the ports of the VLAN. Tagged ports are designated with a "T" and untagged ports with a "U."

Specifying a Management VLAN

The management VLAN is the VLAN through which an AT-9400 Series switch expects to receive management packets. This VLAN is important if you are managing a switch remotely or using the enhanced stacking feature of the switch. For more details about specifying a management VLAN, see Chapter 19, "Port-based and Tagged VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*.

Note

You cannot specify a management VLAN when the switch is operating in a multiple VLAN mode.

To specify the management VLAN, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 90.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 103 on page 272.

4. For the Mgmt. VLAN ID parameter, enter the VID of the VLAN on the switch that you want to function as the management VLAN. The VLAN must already exist on the switch. The default is 1, which is the VID of the Default_VLAN.

5. Click **Apply**.

6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Chapter 18

GARP VLAN Registration Protocol (GVRP)

This chapter contains instructions on how to configure GARP VLAN Registration Protocol (GVRP). This chapter contains the following procedures:

- ❑ "Configuring GVRP" on page 286
- ❑ "Enabling or Disabling GVRP on a Port" on page 288
- ❑ "Displaying the GVRP Configuration" on page 289
- ❑ "Displaying the GVRP Port Configuration" on page 291
- ❑ "Displaying the GVRP Database" on page 292
- ❑ "Displaying the GVRP State Machine" on page 293
- ❑ "Displaying the GVRP Counters" on page 296
- ❑ "Displaying the GIP Connected Ports Ring" on page 300

Note

For background information on GVRP, refer to Chapter 18, "GARP VLAN Registration Protocol," in the *AT-S63 Management Software Menus Interface User's Guide*.

Configuring GVRP

To configure GVRP, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 23 on page 90.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 106.

The screenshot shows a web interface for configuring a network device. At the top, there's a header with 'AT-9424T/SP' and a 'Configuration' title bar. Below the title bar, system information is displayed: 'System Name: Marketing' and 'MAC Addr: 00:30:84:AB:EF:CD'. A sidebar on the left contains navigation links: Home, System, Layer 1, Layer 2 (highlighted), Security, QoS, Help, and Logout. The main content area has tabs for 'MAC Address', 'VLAN', 'GVRP' (selected), 'Spanning Tree', and 'Enhanced Stacking'. The 'GVRP Parameters' section contains two columns of settings. The left column has 'Enable GVRP' (checked), 'Leave Time' (60 CentiSeconds), and 'Join Time' (20 CentiSeconds). The right column has 'Enable GIP' (checked), 'Leave All Time' (1000 CentiSeconds), and 'Apply' and 'Defaults' buttons. Below this is the 'GVRP Port Configuration' section, which shows a grid of 24 ports (01-24) with status indicators. A legend on the right explains the status icons: Port is active (green dot), Port is inactive (grey dot), Port is disabled (X icon), and Port is selected (circle icon). A 'Modify' button is at the bottom of the port configuration section.

Figure 106. GVRP Tab (Configuration)

4. In the GVRP Parameters section, adjust the following parameters as necessary.

Enable GVRP

Click to enable or disable GVRP.

Leave Time

Use this parameter to specify the leave time. The range is 30 to 80 centiseconds and the default is 60 centiseconds.

Join Time

Use this parameter to specify the join time. The range is 10 to 60 centiseconds and the default is 20 centiseconds.

Enable GIP

Click to enable GIP, which is required to propagate VLAN information among the ports of the switch.

Leave All Time

The range is 500 to 300 centiseconds and the default is 1000 centiseconds.

5. Click **Apply**.

Configuration changes are immediately activated on the switch.

6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Enabling or Disabling GVRP on a Port

To enable or disable GVRP on a port, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 23 on page 90.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 106 on page 286.

4. In the GVRP Port Configuration section, click the ports that you want to configure.

5. Click **Modify**.

The GVRP Port Configuration page is shown in Figure 107.

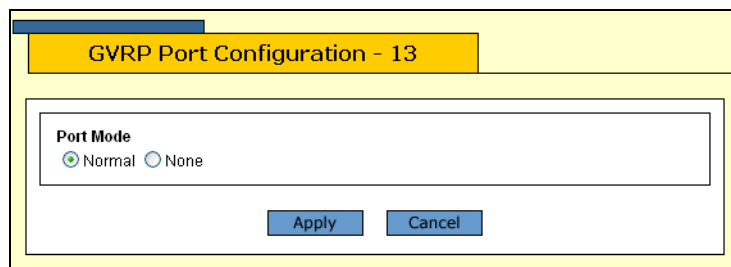


Figure 107. GVRP Port Configuration Page

6. Click **Normal** to have the port propagate GVRP information, or **None** to prevent processing GVRP information and transmitting PDUs.
7. Click **Apply** to save the change, or **Cancel** to cancel.

Displaying the GVRP Configuration

To display the GVRP configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 108.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

Home System Layer 1 Layer 2 Security QoS Help Logout

MAC Address VLAN GVRP Spanning Tree Port Security Enhanced Stacking

GVRP Parameters

<p>GVRP is Disabled</p> <p>Leave Time 60 CentiSeconds</p> <p>Join Time 20 CentiSeconds</p>	<p>GIP is Enabled</p> <p>Leave All Time 1000 CentiSeconds</p>
---	---

View GVRP Parameters

☒ View Port Configuration
 ☐ View GVRP Counters
 ☐ View GVRP Database
 ☐ View GIP Connected Ports Ring
 ☐ View GVRP State Machine for VLAN

Figure 108. GVRP Tab (Monitoring)

The GVRP Parameters section provides the following information:

GVRP

The GVRP status, Enabled or Disabled.

Leave Time

The range is 30 to 80 centiseconds and the default is 60 centiseconds.

Join Time

The range is 10 to 60 centiseconds and the default is 20 centiseconds.

GIP

The GIP status, Enabled or Disabled.

Leave All Time

The range is 500 to 300 centiseconds and the default is 1000 centiseconds.

Displaying the GVRP Port Configuration

To display the GVRP port configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

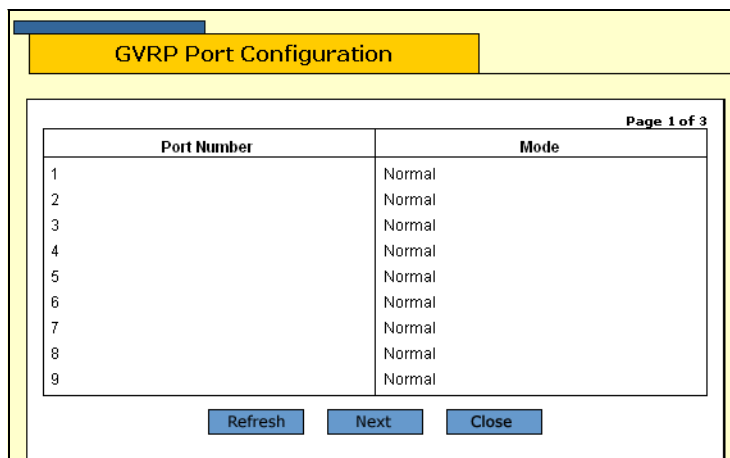
3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 108 on page 289.

4. In the View GVRP Parameters section, click **View Port Configuration**.

5. Click **View**.

The GVRP Port Configuration page is shown in Figure 109.



Port Number	Mode
1	Normal
2	Normal
3	Normal
4	Normal
5	Normal
6	Normal
7	Normal
8	Normal
9	Normal

Page 1 of 3

Refresh Next Close

Figure 109. GVRP Port Configuration Page

The GVRP Port Configuration page provides the following information:

Port Number

The port number.

Mode

The port mode, either Normal or None.

Displaying the GVRP Database

To display the GVRP database, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

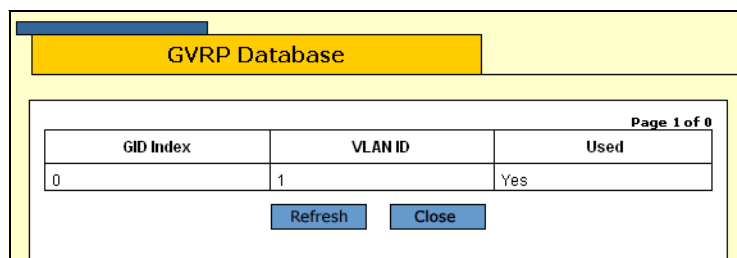
3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 108 on page 289.

4. In the View GVRP Parameters section, click **View GVRP Database**.

5. Click **View**.

The GVRP Database page is shown in Figure 110.



GID Index	VLAN ID	Used
0	1	Yes

Page 1 of 0

Refresh Close

Figure 110. GVRP Database Page

The GVRP Database page provides the following information:

GID Index

The value of the GID index corresponding to the attribute.

VLAN ID

The value of the attribute.

Used

Whether the GID index is currently being used by any port in the GARP application.

Displaying the GVRP State Machine

To display the GVRP state machine, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 108 on page 289.

4. In the View GVRP Parameters section, click **View GVRP State Machine for VLAN** and enter the VLAN number in the box.

5. Click **View**.

The GVRP State Machine for VLAN page is shown in Figure 111.

GVRP State Machine for Vlan - 1											
Port	App.	Reg.	Port	App.	Reg.	Port	App.	Reg.	Port	App.	Reg.
1	Aa	Fix	2	Aa	Fix	3	Aa	Fix	4	Aa	Fix
5	Aa	Fix	6	Aa	Fix	7	Aa	Fix	8	Aa	Fix
9	Aa	Fix	10	Aa	Fix	11	Aa	Fix	12	Aa	Fix
13	Aa	Fix	14	Aa	Fix	15	Aa	Fix	16	Aa	Fix
17	Aa	Fix	18	Aa	Fix	19	Aa	Fix	20	Aa	Fix
21	Aa	Fix	22	Aa	Fix	23	Aa	Fix	24	Aa	Fix

Figure 111. GVRP State Machine for VLAN Page

The GVRP State Machine for VLAN page provides the information shown in Table 7.

Table 7. GVRP State Machine Parameters

Parameter	Meaning
Port	Port number on the switch; this port belongs to the GARP application. If the GARP application has no ports, "No ports have been assigned" is displayed.

Table 7. GVRP State Machine Parameters (Continued)

Parameter	Meaning
App	Applicant state machine for the GID index on that particular port. One of:
	<i>Normal Participant Management state:</i>
	"Vo" Very Anxious Observer
	"Ao" Anxious Observer
	"Qo" Quiet Observer
	"Lo" Leaving Observer
	"Vp" Very Anxious Passive Member
	"Ap" Anxious Passive Member
	"Qp" Quiet Passive Member
	"Va" Very Anxious Active Member
	"Aa" Anxious Active Member
	"Qa" Quiet Active Member
	"La" Leaving Active Member

Table 7. GVRP State Machine Parameters (Continued)

Parameter	Meaning	
App (Continued)	<i>Non-Participant Management state:</i>	
	"Von"	Very Anxious Observer
	"Aon"	Anxious Observer
	"Qon"	Quiet Observer
	"Lon"	Leaving Observer
	"Vpn"	Very Anxious Passive Member
	"Apn"	Anxious Passive Member
	"Qpn"	Quiet Passive Member
	"Van"	Very Anxious Active Member
	"Aan"	Anxious Active Member
	"Qan"	Quiet Active Member
	"Lan"	Leaving Active Member
	The initialized state for the Applicant is Vo.	
Reg	Registrar state machine for the GID index on that particular port. One of:	
	"Mt"	Empty
	"Lv3"	Leaving substate 3 (final Leaving substate)
	"Lv2"	Leaving substate 2
	"Lv1"	Leaving substate 1
	"Lv"	Leaving substate (initial Leaving substate)
	"In"	In
	"Fix"	Registration Fixed
	"For"	Registration Forbidden
	The initialized state for the Registrar is Mt.	

Displaying the GVRP Counters

To display the GVRP counters, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 108 on page 289.

4. In the View GVRP Parameters section, click **View GVRP Counters**.

5. Click **View**.

The GVRP Counters page is shown in Figure 112.

GVRP Counters			
Receive		Transmit	
Total GARP Packets	0	Total GARP Packets	0
Invalid GARP Packets	0		
Discarded			
GARP Disabled	0	GARP Disabled	24
Port Not Listening	0	Port Not Sending	0
Invalid Port	0		
Invalid Protocol	0		
Invalid Format	0		
Database Full	0		
GARP Messages			
LeaveAll	0	LeaveAll	0
JoinEmpty	0	JoinEmpty	0
JoinIn	0	JoinIn	0
LeaveEmpty	0	LeaveEmpty	0
LeaveIn	0	LeaveIn	0
Empty	0	Empty	0
Bad Message	0		
Bad Attribute	0		

Refresh
Close

Figure 112. GVRP Counters Page

The GVRP Counters page provides the information shown in Table 8.

Table 8. GVRP Counters

Parameter	Meaning
Receive: Total GARP Packets	Total number of GARP PDUs received by this GARP application.
Transmit: Total GARP Packets	Total number of GARP PDUs transmitted by this GARP application.
Receive: Invalid GARP Packets	Number of invalid GARP PDUs received by this GARP application.
Receive Discarded: GARP Disabled	Number of received GARP PDUs discarded because the GARP application was disabled.
Transmit Discarded: GARP Disabled	Number of GARP PDUs discarded because the GARP application was disabled. This counter is incremented when ports are added to or deleted from the GARP application arising from port movements in the underlying VLAN or STP.
Receive Discarded: Port Not Listening	Number of GARP PDUs discarded because the port that received the PDUs was not listening, that is, MODE=NONE was set on the port.
Transmit Discarded: Port Not Sending	Number of GARP PDUs discarded because the port that the PDUs were to be transmitted on was not sending, that is, MODE=NONE was set on the port.
Receive Discarded: Invalid Port	Number of GARP PDUs discarded because the port that received the PDU does not belong to the GARP application.
Receive Discarded: Invalid Protocol	Number of GARP PDUs discarded because the GARP PDU contained an invalid protocol.
Receive Discarded: Invalid Format	Number of GARP PDUs discarded because the format of the GARP PDU was not recognized.
Receive Discarded: Database Full	Number of GARP PDUs discarded because the database for the GARP application was full, that is, the maximum number of attributes for the GARP application is in use.

Table 8. GVRP Counters (Continued)

Parameter	Meaning
Receive GARP Messages: LeaveAll	Number of GARP LeaveAll messages received by the GARP application.
Transmit: GARP Messages: LeaveAll	Number of GARP LeaveAll messages transmitted by the GARP application.
Receive GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages received for all attributes in the GARP application.
Transmit GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: JoinIn	Total number of GARP JoinIn messages received for all attributes in the GARP application.
Transmit GARP Messages: JoinIn	Total number of GARP JoinIn messages transmitted for all attributes in the GARP application.
Receive GARP Messages: LeaveEmpty	Total number of GARP LeaveEmpty messages received for all attributes in the GARP application.
Transmit GARP Messages: LeaveEmpty	Total number of GARP LeaveEmpty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: LeaveIn	Total number of GARP LeaveIn messages received for all attributes in the GARP application.
Transmit GARP Messages: LeaveIn	Total number of GARP LeaveIn messages transmitted for all attributes in the GARP application.
Receive GARP Messages: Empty	Total number of GARP Empty messages received for all attributes in the GARP application.
Transmit GARP Messages: Empty	Total number of GARP Empty messages transmitted for all attributes in the GARP application.

Table 8. GVRP Counters (Continued)

Parameter	Meaning
Receive GARP Messages: Bad Message	Number of GARP messages that had an invalid Attribute Type value, an invalid Attribute Length value or an invalid Attribute Event value.
Receive GARP Messages: Bad Attribute	Number of GARP messages that had an invalid Attribute Value value.

Displaying the GIP Connected Ports Ring

To display the GIP connected ports ring, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

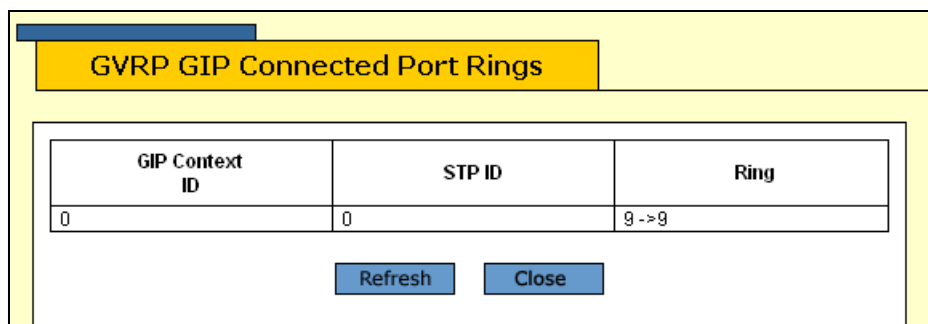
3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 108 on page 289.

4. In the View GVRP Parameters section, click **View GIP Connected Ports Ring**.

5. Click **View**.

The GIP Connected Ports Ring page is shown in Figure 113.



GIP Context ID	STP ID	Ring
0	0	9 -> 9

Refresh Close

Figure 113. GIP Connected Ports Ring Page

The GIP Connected Ports Ring page displays a table that contains the following columns of information:

GIP Context ID

A number assigned to the instance for the GIP context.

STP ID

Present if the GARP application is GVRP; identifies the spanning tree instance associated with the GIP context.

Ring

The ring of connected ports. Only ports presently in the spanning tree Forwarding state are eligible for membership in the GIP

connected ring. If no ports exist in the GIP connected ring, "No ports are connected" is displayed. If the GARP application has no ports, "No ports have been assigned" is displayed.

Section IV

Security

The chapters in this section explain how to set up security on an AT-9400 Series switch. The chapters include:

- ☐ Chapter 19, "Port Security" on page 305
- ☐ Chapter 20, "Encryption Keys, PKI, and SSL" on page 309
- ☐ Chapter 21, "Secure Shell (SSH)" on page 317
- ☐ Chapter 22, "TACACS+ and RADIUS" on page 323
- ☐ Chapter 23, "802.1x Port-based Network Access Control" on page 333
- ☐ Chapter 24, "Denial of Service Defense" on page 351

Chapter 19

Port Security

This chapter explains how to display the MAC address security levels on the ports on the switch. It contains the following section:

- ❑ "Displaying the MAC Address Security Level" on page 306

Note

For background information on port security, refer to Chapter 23, "Port Security," in the *AT-S63 Management Software Menus Interface User's Guide*.

Note

You cannot configure the MAC address security feature using the web browser interface. You can only configure this feature using the menus or CLI interfaces.

Displaying the MAC Address Security Level

To display the MAC address security level of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

3. Select the **Port Security** tab.

The Port Security tab is shown in Figure 114.

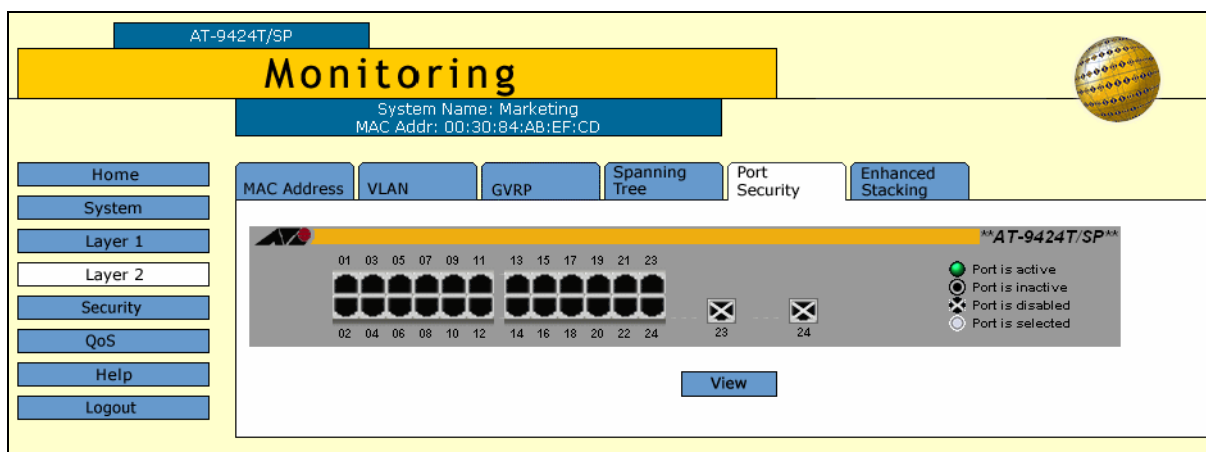


Figure 114. Port Security Tab (Monitoring)

4. Click the port whose port security level you want to view. A selected port turns white. You can select more than one port at a time.
5. Click **View**.

The Security for Port(s) page is shown in Figure 115.

Total Ports Selected: 3. Page 1 of 1				
Port	Security Mode	Intruder Action	Participating	MAC Limit
2	Limited	Send Trap Only	Yes	10
3	Limited	Send Trap Only	Yes	10
4	Limited	Send Trap Only	Yes	10

OK

Figure 115. Security for Port(s) Page

The Security for Ports page displays a table that contains the following columns of information:

Port

The number of the port.

Security Mode

The active security mode on the switch.

Intruder Action

The column specifies the action taken by the switch if a port receives an invalid packet. The possible settings are:

No Action (Discard) - The port discards invalid packets. This is the default.

Trap - The port discards invalid packets and sends a trap.

Trap/Disable - The port discards invalid packets, sends a trap, and disables the port.

Participating

This column applies only when the intrusion action for a port is set to trap or disable. This option does not apply when intrusion action is set to No Action (discard). If this option is set to No when intrusion action is set to trap or disable, the port discards invalid packets, but it does not send a trap or disable the port.

MAC Limit

This column specifies the maximum number of dynamic MAC addresses the port learns. It only applies when a port is operating in the Limited security mode.

Chapter 20

Encryption Keys, PKI, and SSL

This chapter explains how to view the encryption keys, PKI-based certificates, and SSL settings and includes the following sections:

- ❑ "Displaying the Encryption Keys" on page 310
- ❑ "Displaying the PKI Settings and Certificates" on page 312
- ❑ "Displaying the SSL Settings" on page 315

Note

To configure encryption keys, PKI, or SSL, you must use the AT-S63 menus or CLI interface.

For information about or to configure encryption keys using the menus interface, refer to Chapter 26, "Encryption Keys," in the *AT-S63 Management Software Menus Interface User's Guide*. To configure encryption keys using the CLI, refer to Chapter 28, "Encryption Key Commands," in the *AT-S63 Management Software Command Line Interface User's Guide*.

For information about, or to configure PKI and SSL using the menus interface, refer to Chapter 27, "PKI Certificates and SSL" in the *AT-S63 Management Software Menus Interface User's Guide*. To configure PKI using the CLI, refer to Chapter 29, "Public Key Infrastructure (PKI) Certificate Commands," in the *AT-S63 Management Software Command Line Interface User's Guide*. To configure SSL using the CLI, refer to Chapter 30, "Secure Sockets Layer (SSL) Commands," in the *AT-S63 Management Software Command Line Interface User's Guide*.

Displaying the Encryption Keys

To configure the encryption keys, you must use the AT-S63 menus or command line interface. For more information about encryption keys, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

To display the encryption keys, perform the following procedure:

- 1. From the Home page, select **Monitoring**.
The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.
- 2. From the Monitoring menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab displayed by default, as shown in Figure 116.

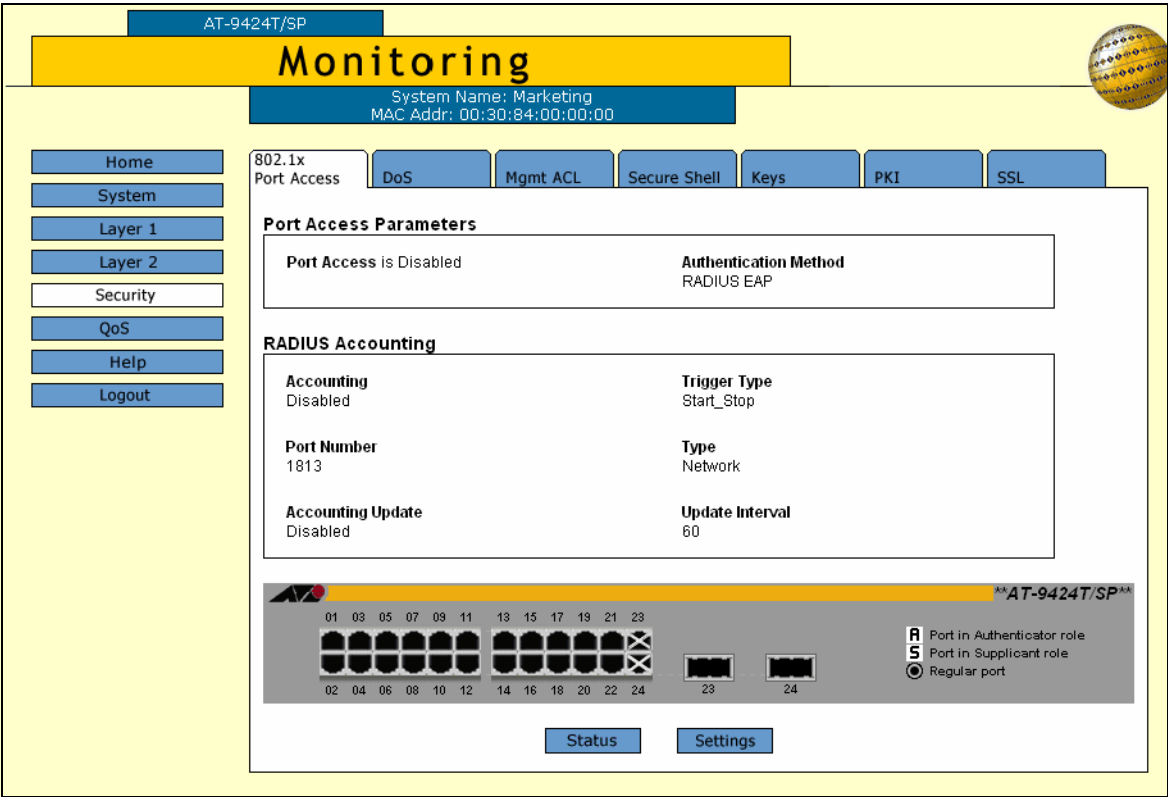


Figure 116. 802.1x Port Access Tab (Monitoring)

- 3. Select the **Keys** tab.

The Keys tab is shown in Figure 117.

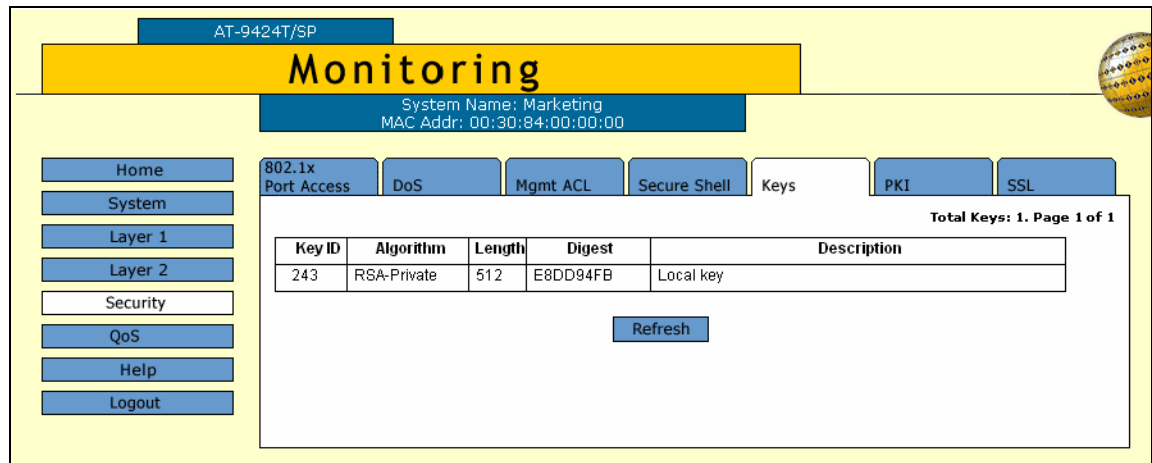


Figure 117. Keys Tab (Monitoring)

The Keys tab displays a table that contains the following columns of information:

ID

The identification number of the key.

Algorithm

The algorithm used in creating the encryption. This is always RSA - Private.

Length

The length of the key in bits.

Digest

The CRC32 value of the MD5 digest of the public key.

Description

The key's description.

You use these keys when you configure Secure Sockets Layer (SSL) or Secure Shell (SSH). To configure SSL you must use the AT-S63 menus or CLI interface. To configure SSH, refer to Chapter 21, "Secure Shell (SSH)" on page 317.

Displaying the PKI Settings and Certificates

You can view the current PKI settings and certificates on the switch. To configure the PKI settings and certificates, you must use the AT-S63 menus or command line interface. For more information about PKI, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

To display the PKI settings and certificates, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab displayed by default, as shown in Figure 116 on page 310.

3. Select the **PKI** tab.

The PKI tab is shown in Figure 118.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

802.1x Port Access DoS Mgmt ACL Secure Shell Keys PKI SSL

Maximum Number of Certificates is 256

Total Certificates: 2, Page 1 of 1

	Name	State	MTrust	Type	Source
<input checked="" type="radio"/>	Local	Trusted	True	EE	Command
<input type="radio"/>	Secondary	Trusted	True	EE	Command

Refresh View

Figure 118. PKI Tab (Monitoring)

The upper section states the maximum number of certificates that can be configured on the switch.

The lower section displays a table that lists the currently configured certificates and contains the following columns of information:

Name

The certificate name.

State

The state of the certificate, one of the following:

Trusted - The certificate is from a trusted CA.

Untrusted - The certificate is from an untrusted CA.

MTrust (Manually Trusted)

The certificate has been manually verified that it is from a trusted or untrusted authority.

Type

The certificate type, one of the following:

EE - The certificate was issued by a CA.

CA - The certificate belongs to a CA.

Self - A self-signed certificate.

Source

The certificate was created on the switch.

4. To view the details about a certificate, click the certificate and click **View**.

The X509 Certificate Details page is shown in Figure 119.

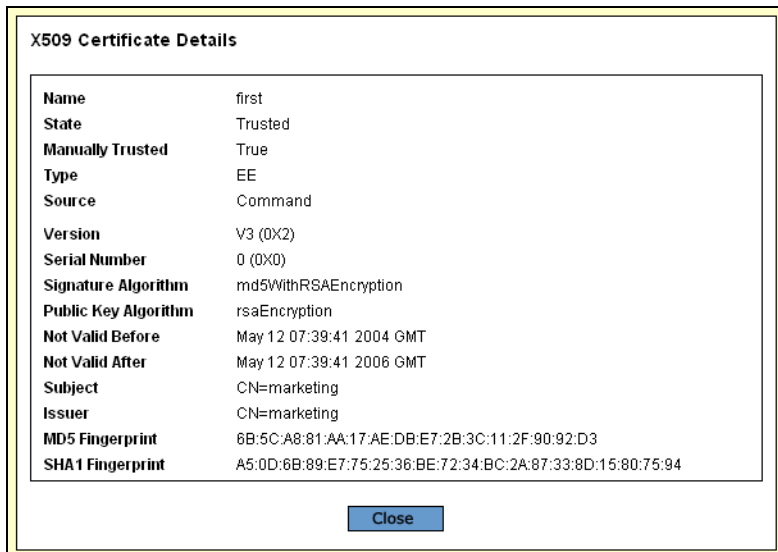


Figure 119. X509 Certificate Details Page

The X509 Certificate Details page provides the following information about the certificate:

Name

The name of the certificate.

State

Whether the certificate is Trusted or Untrusted.

Manually Trusted

You verified the certificate is from a trusted or untrusted authority.

Type

The type of the certificate. The options are EE, SELF, and CA.

Source

The certificate was created on the switch.

Version

The version number of the AT-S63 management software.

Serial Number

The certificate's serial number.

Signature Algorithm

The signature algorithm of the certificate.

Public Key Algorithm

The public key algorithm.

Not Valid Before

The date the certificate became active.

Not Valid After

The date the certificate expires. Self-signed certificates are valid for two years.

Subject

The Subject distinguished name.

Issuer

The certificate issuer's distinguished name.

MD5 Fingerprint

The MD5 algorithm. This value provides a unique sequence for each certificate consisting of 16 bytes.

SHA1 Fingerprint

The Secure Hash Algorithm. This value provides a unique sequence for each certificate consisting of 20 bytes.

5. Click **Close** to close the page.

Displaying the SSL Settings

To configure the SSL settings, you must use the AT-S63 menus or command line interface. For information, refer to the *AT-S63 Management Software Menus Interface User's Guide* and the *AT-S63 Management Software Command Line Interface User's Guide*.

To display the SSL settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab displayed by default, as shown in Figure 116 on page 310.

3. Select the **SSL** tab.

The SSL tab is shown in Figure 117.

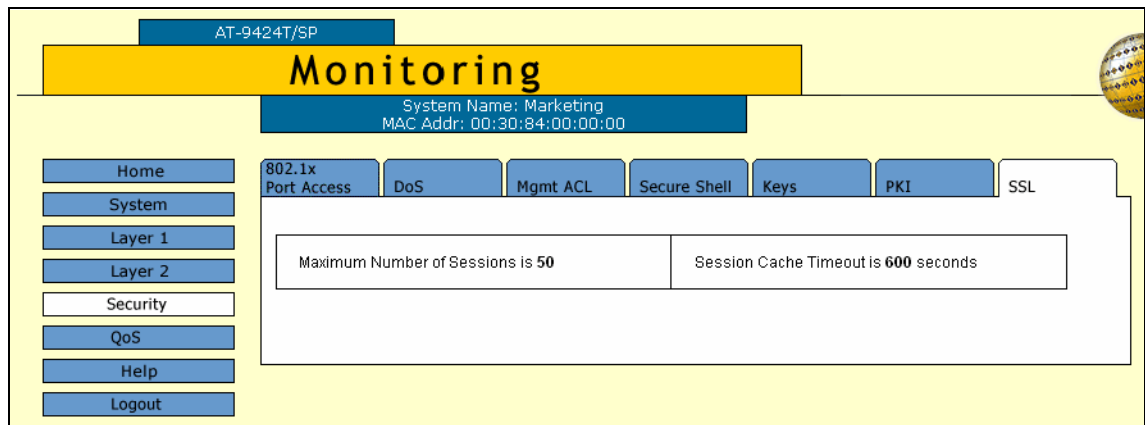


Figure 120. SSL Tab (Monitoring)

The SSL tab provides the following information:

Maximum Number of Sessions

The maximum number of SSL sessions allowed at one time.

Session Cache Timeout

The length of time before the session cache times out, in seconds.

Chapter 21

Secure Shell (SSH)

This chapter explains how to configure the Secure Shell (SSH) protocol and contains the following sections:

- ❑ "Configuring SSH" on page 318
- ❑ "Displaying the SSH Settings" on page 320

Note

For background information on SSH, refer to Chapter 28, "Secure Shell (SSH)," in the *AT-S63 Management Software Menus Interface User's Guide*.

Configuring SSH

To display the MAC address security level of a port, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Configuration menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab displayed by default, as shown in Figure 129 on page 334.

3. Select the **Secure Shell** tab.

The Secure Shell tab is shown in Figure 121.

The screenshot shows the 'Configuration' page for a device (AT-9424T/SP). The 'Secure Shell' tab is selected. The configuration area is titled 'Secure Shell Configuration' and contains the following fields:

- Status:** Radio buttons for 'Disabled' (selected) and 'Enabled'.
- Key ID:** Text field with 'Not Defined' and a note '[Key Size: 1024 Bits]'.
- Server Key ID:** Text field with 'Not Defined' and a note '[Key Size: 768 Bits]'.
- Server Expiry Time:** Text field with '0' and a note 'hours [0-5]'.
- Login Timeout:** Text field with '180' and a note 'seconds [60-600]'.

An 'Apply' button is located at the bottom right of the configuration area.

Figure 121. Secure Shell Tab (Configuration)

4. Adjust the following parameters as necessary:

Key ID

Enter a host key ID. The default is Not Defined. Enter a value that you configured in the encryption menus using the AT-S63 menus interface.

Server Key ID

Enter a server key ID. The default is Not Defined. Enter a value that you configured in the encryption menus using the AT-S63 menus interface.

Server Expiry Time

Set the time, in hours, for the server key to expire.

This timer determines how often the server key is regenerated. A server key is regenerated for security purposes. A server key is only valid for the time period configured in the Server Key Expiry (Expiration) Time timer. Allied Telesyn recommends that you set this field to 1. With this setting, a new key is generated every hour.

Login Timeout

Enter a number between 60 and 600. The default is 180.

This is the time it takes to release the SSH server from an incomplete SSH client connection. Enter a time in seconds. The default is 180 seconds (3 minutes). The range is 60 to 600 seconds.

Status

Enable the SSH server after you have finished the configuration and want to log on to the server. Or, click Disabled while you are configuring the protocol. SSH must be disabled while you are configuring the protocol. This is the default.

5. Click **Apply**.
6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying the SSH Settings

To view the Secure Shell settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Configuration menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab displayed by default, as shown in Figure 6 on page 44.

3. Select the **Secure Shell** tab.

The Secure Shell tab is shown in Figure 122.

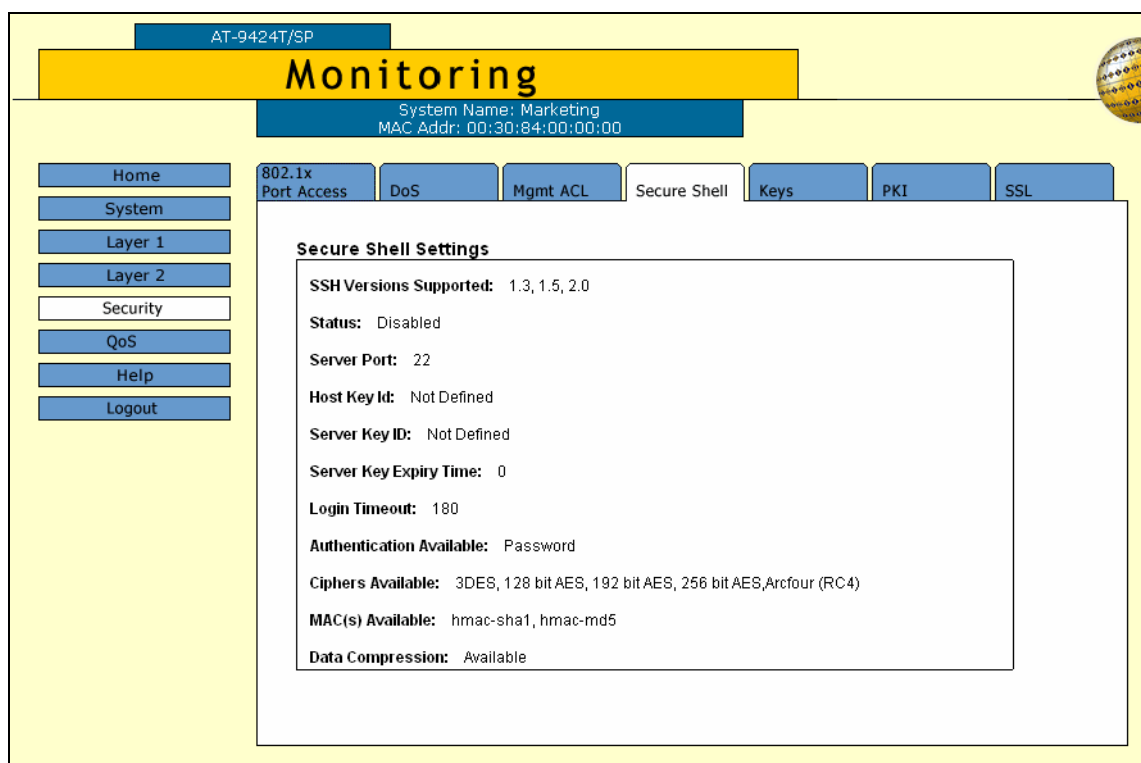


Figure 122. Secure Shell Tab (Monitoring)

The Secure Shell tab provides the following information:

SSH Versions Supported

The versions of SSH which are supported by the AT-S63 management software.

Status

Whether or not the SSH server is enabled or disabled.

Server Port

The well-known port for SSH. The default is port 22.

Host Key ID

The host key ID defined for SSH.

Server Key ID

Server key ID defined for SSH.

Server Key Expiry Time

Length of time, in hours, until the server key is regenerated. The default is 0 hours which means the server key is not regenerated.

Login Timeout

Time, in seconds, until a SSH server is released from an incomplete connection with a SSH client.

Authentication Available

Authentication method available. Currently, password authentication is the only supported method.

Ciphers Available

SSH ciphers that are available on the switch.

MACs Available

Message Authorization Code (MAC) that is used to validate incoming SSH messages to the server. Two algorithms are supported.

Data Compression

Whether or not data compression is available on the switch. Data compression is useful for networks that have a slow throughput speed.

Chapter 22

TACACS+ and RADIUS

This chapter contains instructions on how to configure the authentication protocols. This chapter contains the following procedures:

- ❑ "Enabling or Disabling TACACS+ or RADIUS" on page 324
- ❑ "Configuring TACACS+" on page 325
- ❑ "Displaying the TACACS+ Settings" on page 327
- ❑ "Configuring RADIUS" on page 329
- ❑ "Displaying the RADIUS Settings" on page 331

Note

For background information on the authentication protocols, refer to Chapter 30, "TACACS+ and RADIUS," in the *AT-S63 Management Software Menus Interface User's Guide*.

Enabling or Disabling TACACS+ or RADIUS

To enable or disable the authentication protocols, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40

2. Select the **Server-based Authentication** tab.

The Server-based Authentication tab is shown in Figure 123.

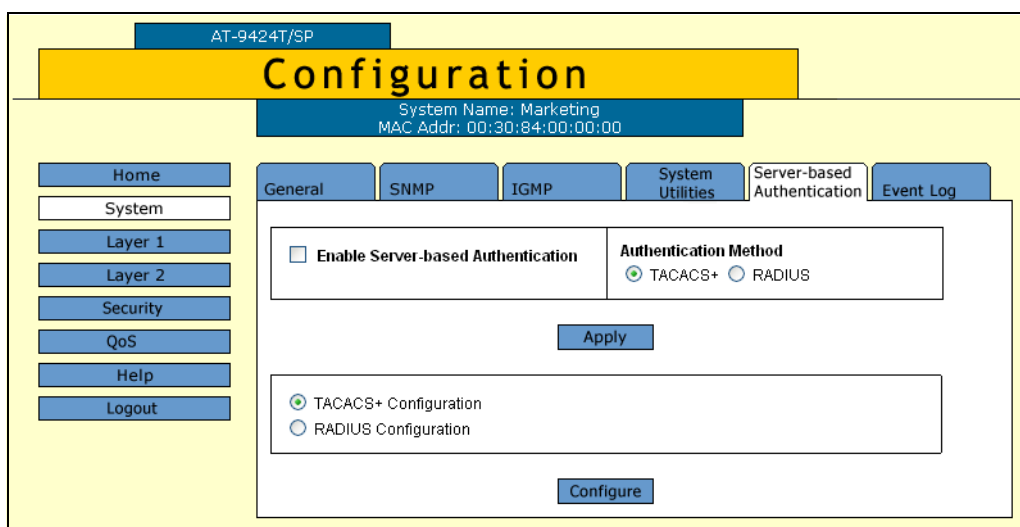


Figure 123. Server-based Authentication Tab (Configuration)

3. To select an authentication protocol, in the Authentication Method section of the tab, click either RADIUS or TACACS+. The default is TACACS+.

Note

The switch can support only one authentication protocol at a time. Additionally, you cannot select a different authenticator protocol when this feature is enabled.

4. To enable or disable the authentication feature on the switch, click the Enable Server-based Authentication check box. A check in the box indicates that this feature is enabled. No check indicate the feature is disabled. The default is disabled.
5. Click **Apply**.

To configure TACACS+, go to "Configuring TACACS+", next. To configure RADIUS, go to "Configuring RADIUS" on page 329-.

Configuring TACACS+

To configure TACACS+, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40

2. Select the **Server-based Authentication** tab.

The Server-based Authentication tab is shown in Figure 123 on page 324.

3. In lower section of the Server-based Authentication tab, click TACACS+ Configuration and click **Configure**.

The TACACS+ Client Configuration page is shown in Figure 124.

Server #	IP Address	Encryption Key
1	0.0.0.0	
2	0.0.0.0	
3	0.0.0.0	

Figure 124. TACACS+ Client Configuration Page

4. Adjust the following parameters as necessary.

Global Secret

If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

Global Server Timeout

This parameter specifies the maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server cannot respond. If the timeout expires and the server has

not responded, the switch queries the next TACACS+ server in the list. If there are no more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address and Encryption Key

Use these fields to specify the IP addresses and encryption secrets of up to three network servers containing TACACS+ server software. You can leave an encryption field blank if you entered the server's secret in the Global Secret field.

5. Click **Apply**.
6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying the TACACS+ Settings

To display the TACACS+ settings on the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **Server-based Authentication** tab.

The Server-based Authentication tab is shown in Figure 125.

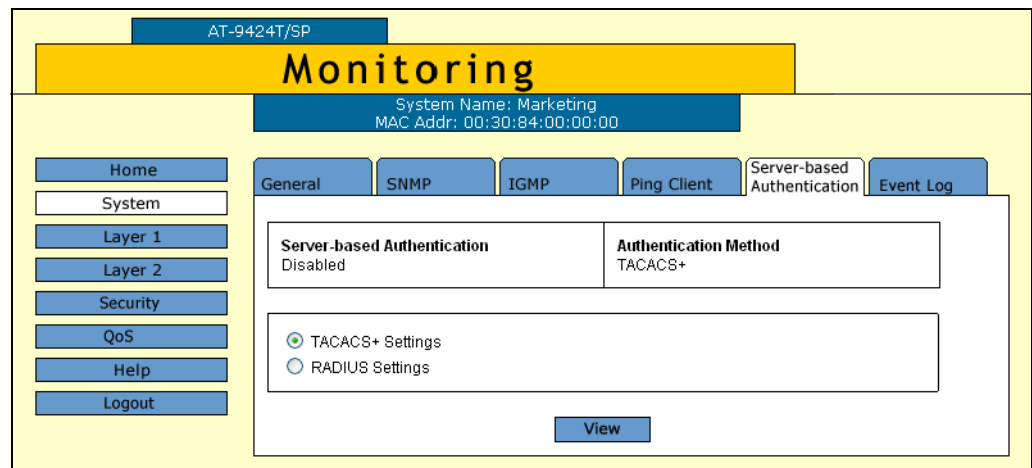


Figure 125. Server-Based Authentication Tab (Monitoring)

The upper part of the page shows if server-based authentication is enabled or disabled and the authentication method. The lower part of the page allows you to view either the settings for the current authentication method.

3. In the lower portion of the tab, click TACACS+ Settings.
4. Click **View**.

The TACACS+ client configuration page is shown in Figure 126.

TACACS+ Client Configuration		
Global Secret Winner		Global Server Timeout [1-300] 30 second(s)
Server #	IP Address	Encryption Key
1	149.32.14.237	RC Corp.
2	149.32.14.248	RC Corp.
3	149.32.14.248	
Cancel		

Figure 126. TACACS+ Client Configuration Page

The upper portion of the page provides the following information:

Global Secret

The TACACS+ server encryption secret.

Global Server Timeout

The maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server cannot respond.

The lower portion of the page displays a table that contains the following columns of information:

Server #

The server number, one of three.

IP Address

IP addresses of up a network server containing TACACS+ server software.

Encryption Key

Encryption key for the server. This parameter is blank if all the TACACS+ servers have the same encryption secret.

Configuring RADIUS

To configure RADIUS, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40

2. Select the **Server-based Authentication** tab.

The Server-based Authentication tab is shown in Figure 123 on page 324.

3. In lower section of the Server-based Authentication tab, click RADIUS Configuration and click **Configure**.

The RADIUS Client Configuration page is shown in Figure 124.

Server No.	IP Address	Port # [1-65535]	Encryption Key
1	0.0.0.0	1812	[Not Defined]
2	0.0.0.0	1812	[Not Defined]
3	0.0.0.0	1812	[Not Defined]

Figure 127. RADIUS Client Configuration Page

4. Adjust the following parameters as necessary.

Global Encryption Key

If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

Global Server Timeout

This parameter specifies the maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server cannot respond. If the timeout expires and the server has

not responded, the switch queries the next TACACS+ server in the list. If there no more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address, Port #, and Encryption Key

Use these fields to specify the IP address, UDP port number, and encryption key of each RADIUS server. You can specify up to a maximum of three servers. You can leave the encryption field blank if you entered the server's key in the Global Secret field.

5. Click **Apply**.
6. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying the RADIUS Settings

To display the RADIUS settings on the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **Server-based Authentication** tab.

The Server-based Authentication tab is shown in Figure 125 on page 327. The upper part of the page shows if server-based authentication is enabled or disabled and the authentication method. The lower part of the page allows you to view either the settings for the current authentication method.

3. In the lower portion of the page, click RADIUS Settings.
4. Click **View**.

The RADIUS Client Configuration page is shown in Figure 126.

Server No.	IP Address	Port # [1-65535]	Encryption Key
1	149.11.11.11	1812	s24aa
2	149.22.22.22	1812	s45nnn
3	0.0.0.0	1812	[Not Defined]

Figure 128. RADIUS Client Configuration Page

The upper portion of the page displays the following information:

Global Encryption Key

The global encryption secret.

Global Server Timeout

The maximum amount of time the switch waits for a response from a RADIUS server before assuming the server cannot respond.

The lower portion of the page displays a table that contains the following columns of information:

Server #

The server number, one of three.

IP Address

IP address of the RADIUS server.

Port

Port of the RADIUS server.

Encryption Key

Encryption key for that server. This parameter is blank if all the RADIUS servers have the same encryption secret.

Chapter 23

802.1x Port-based Network Access Control

This chapter contains instructions on how to configure the 802.1x Port-based Network Access Control feature on the switch. The chapter contains the following sections:

- ❑ "Setting Port Roles" on page 334
- ❑ "Enabling or Disabling 802.1x Port-based Network Access Control" on page 336
- ❑ "Configuring Authenticator Port Parameters" on page 337
- ❑ "Configuring Supplicant Port Parameters" on page 340
- ❑ "Displaying the Port-based Network Access Control Parameters" on page 342
- ❑ "RADIUS Accounting" on page 346

Note

For background information on port-based network access control, refer to Chapter 29, "802.1x Port-based Network Access Control," in the *AT-S63 Management Software Menus Interface User's Guide*.

Setting Port Roles

To set port roles for port-based network access control, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 129.

The screenshot displays the 'Configuration' page for an AT-9424T/SP switch. The '802.1x Port Access' tab is selected. The page includes a sidebar with navigation links: Home, System, Layer 1, Layer 2, Security (selected), QoS, Help, and Logout. The main content area is divided into two sections: 'Configure Port Access Parameters' and 'Configure RADIUS Accounting'. The 'Configure Port Access Parameters' section has a checkbox for 'Enable Port Access' (unchecked), an 'Authentication Method' dropdown set to 'RADIUS EAP', and an 'Apply' button. The 'Configure RADIUS Accounting' section has a checkbox for 'Enable Accounting' (unchecked), a 'Trigger Type' dropdown set to 'Start Stop', a 'Port Number' input field with '1813', a 'Type' dropdown set to 'Network', a checkbox for 'Enable Update' (unchecked), an 'Update Interval' input field with '60', and an 'Apply' button. At the bottom, there is a graphical representation of the switch ports (01-24) with a legend indicating 'A' for Port in Authenticator role, 'S' for Port in Supplicant role, and a black circle for Regular port. The ports are currently all black, indicating they are regular ports. There are also 'Port Role' and 'Settings' buttons at the bottom.

Figure 129. 802.1x Port Access Tab (Configuration)

The graphical image of the switch shows which ports have already been assigned port roles. An "A" indicates that a port is functioning as an authenticator while an "S" indicates the port is functioning as a supplicant. A black port has not been assigned a port role and is not participating in port-based access control. This is the default setting for a port.

3. To set a port's role, click on the port. The selected port turns white. You can select more than one port at a time.
4. Click **Port Role**.

The Port Role Configuration page is shown in Figure 130.

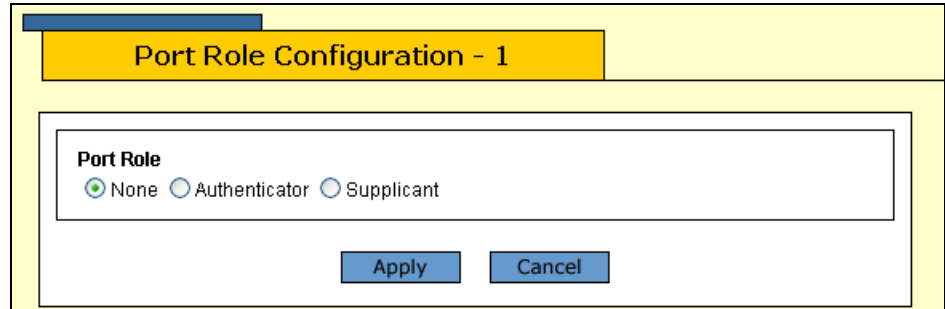


Figure 130. Port Role Configuration Page

5. Select the desired role for the port. The possible settings are:

None

The port is not to participate in port-based access control. This is the default setting.

Authenticator

The port is to function as an authenticator. This is the appropriate setting if the port is connected to a supplicant.

Supplicant

The port is to function as an supplicant. This is the appropriate setting if the port is connected to an authenticator. A port can have only one port role at a time.

6. Click **Apply**.

To enable or disable port-based access control, go to "Enabling or Disabling 802.1x Port-based Network Access Control" on page 336. Then, to configure authenticator port settings, go to "Configuring Authenticator Port Parameters" on page 337. To configure supplicant port settings, go to "Configuring Supplicant Port Parameters" on page 340.

Enabling or Disabling 802.1x Port-based Network Access Control

To enable or disable 802.1x Port-based Network Access Control, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 129 on page 334.

You cannot change the Authentication Method field.

3. Click the **Enable Port Access** check box. A check in the box means that the feature is activated on the switch. No check means that the feature is disabled.

4. Click **Apply**.

5. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Configuring Authenticator Port Parameters

To configure authenticator port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 129 on page 334.

3. Click the authenticator port that you want to configure. You can select more than one authenticator port at a time. The selected port turns white.

Note

A port must already be configured as an authenticator before you can configure its settings. For instructions on how to set the role of a port, refer to "Setting Port Roles" on page 334.

4. Click **Settings**.

The Authenticator Parameters page is shown in Figure 131.

Authenticator Parameters - 6	
Port Control Auto	Quiet Period 60
Tx Period 30	Reauth Period 3600
Supplicant Timeout 30	Server Timeout 30
Max Requests 2	
Apply Close	

Figure 131. Authenticator Parameters Page

5. Adjust the following parameters as necessary:

Port Control

The possible settings are:

Force-authorized - Disables IEEE 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default setting

Force-unauthorized - Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface

Auto - Enables 802.1x port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client that attempts to access the network is uniquely identified by the switch using the client's MAC address.

Quiet Period

Sets the number of seconds that the port remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

TX Period

Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

Reauth Period

Enables periodic reauthentication of the client, which is disabled by default. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

Supplicant Timeout

Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

Server Timeout

Sets the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 10 seconds. The range is 1 to 60 seconds.

Max Requests

Specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

6. Click **Apply**.
7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Configuring Supplicant Port Parameters

To configure supplicant port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 129 on page 334.

3. Click the supplicant port that you want to configure. You can select more than one supplicant port at a time. The selected port turns white.

Note

A port must already be designated as a supplicant before you can configure its settings. For instructions on how to set the role of a port, refer to "Setting Port Roles" on page 334.

4. Click **Settings**.

The Supplicant Parameters page is shown in Figure 131.

Supplicant Parameters - 20	
Auth Period <input type="text" value="30"/>	Held Period <input type="text" value="60"/>
Max Start <input type="text" value="3"/>	Start Period <input type="text" value="30"/>
User Name <input type="text"/>	User Password <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Close"/>	

Figure 132. Supplicant Parameters Page

5. Adjust the following parameters as needed:

Auth Period

Specifies the period of time in seconds that the supplicant waits for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 60 seconds. The default is 30 seconds.

Held Period

Specifies the amount of time in seconds the supplicant is to refrain from retrying to re-contact the authenticator in the event the end user provides an invalid username and/or password. After the time period has expired, the supplicant can attempt to log on again. The range is 0 to 65,535 seconds. The default value is 60 seconds.

Max Start

Specifies the maximum number of times the supplicant sends EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

Start Period

Specifies the time period in seconds between successive attempts by the supplicant to establish contact with an authenticator when there is no reply. The range is 1 to 60. The default is 30.

User Name

Specifies the username for the switch port. The port sends the name to the authentication server for verification when the port logs on to the network. The username can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The username is case sensitive.

User Password

Specifies the password for the switch port. The port sends the password to the authentication server for verification when the port logs on to the network. The password can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The password is case sensitive.

6. Click **Apply**.
7. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying the Port-based Network Access Control Parameters

You can display information about the port-based network access control status and settings of the ports on the switch. This section contains the following procedures:

- ❑ "Displaying the Port Status" (next)
- ❑ "Displaying the Port Settings" on page 343

Displaying the Port Status

To display the port-based network access control port status, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Security** option.

The Security page opens with the 802.1x Port Access tab selected by default, as shown in Figure 133.

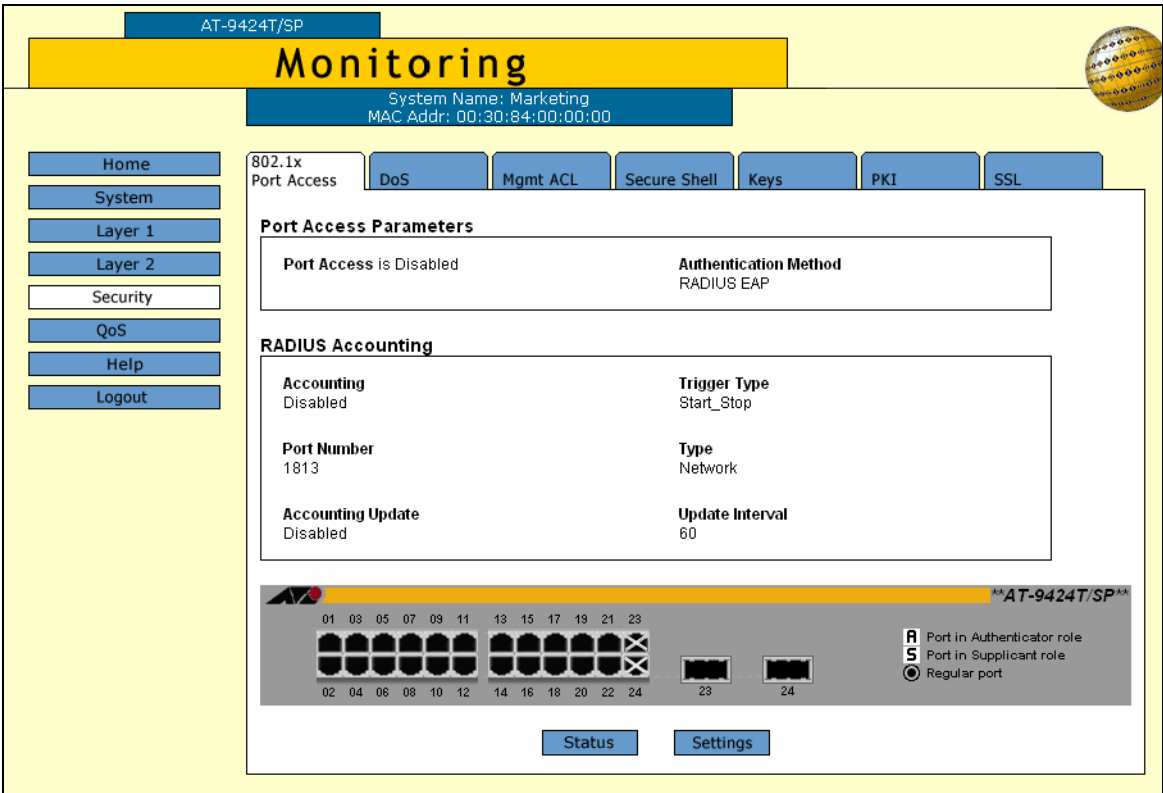


Figure 133. 802.1x Port Access Tab (Monitoring)

- To see the status of the port, click the port and click **Status**. You can select more than one port at a time.

The Port Access Port Status page is shown in Figure 134.

Port	Port Role	Status	Additional Info.
8	Authenticator	-----	-----

OK

Figure 134. Port Access Port Status Page

The Port Access Port Status page displays a table that contains the following columns of information:

Port

The port number.

Port Role

The port role: None, Authenticator, or Supplicant.

Status

The options include: Initialize, Disconnected, and so forth.

Additional Info.

More information about the port including the MAC address.

Displaying the Port Settings

To display the port-based network access control port settings, perform the following procedure:

- From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

- From the Monitoring menu, select the **Security** option.

The Security page opens with the 802.1x Port Access tab selected by default, as shown in Figure 133 on page 342.

- To review the port access settings, click OK to close the Port Access Port Status page and return to the 802.1x Port Access tab
- To see the port settings, click the port and click **Settings**. You can select more than one port at a time.

Note

To view the settings of multiple ports, you must select ports that have the same port role (authenticator or supplicant).

For authenticator port(s), the Authenticator Port Parameters page is displayed, as shown in Figure 135.

Port	PortCtrl	QuietP	TxP	ReAuthP	SuppTO	SvrTO	MaxReq
8	Auto	60	30	3600	30	30	2

OK

Total Ports = 1, Page 1 of 1

Figure 135. Authenticator Port Parameters Page

The Authenticator Port Parameters page displays a table that contains the following columns of information:

Port

The port number.

PortCtrl

The port control setting. The possible settings are:

Force-authorized - 802.1x port-based authentication is disabled.

Force-unauthorized - The port is in an unauthorized state, ignoring attempts by the client to authenticate.

Auto - 802.1x port-based authentication is enabled.

QuietP

The number of seconds the port remains in a quiet state following a failed authentication exchange with the client.

TxP

The number of seconds that the switch waits for a response to an EAP Request packet/identity packet from the client before retransmitting the request.

ReAuthP

The frequency of the periodic reauthentication of the client.

SuppTO

The switch-to-client retransmission time for the EAP Request packet.

MaxReq

The maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session.

For supplicant port(s), the Supplicant Port Parameters Page is displayed, as shown in Figure 136.

Total Ports = 1. Page 1 of 1						
Port	AuthPeriod	HeldPeriod	MaxStart	StartPeriod	User Name	User Password
11	30	60	3	30		

OK

Figure 136. Supplicant Port Parameters Page

The Supplicant Port Parameters page displays a table that contains the following columns of information:

Port

The port number.

AuthPeriod

The period of time in seconds that the supplicant waits for a reply from the authenticator.

HeldPeriod

The amount of time the supplicant is to refrain from trying to recontact the authenticator in the event that the end user provides an invalid user name and/or password.

MaxStart

The maximum number of times the supplicant sends EAPoL-Start packets before assuming that there is no authenticator present.

StartPeriod

The time period between successive attempts by the supplicant to establish contact with an authenticator when there is no reply.

User Name

The user name for the port.

User Password

The password for the port.

RADIUS Accounting

The AT-S63 management software supports RADIUS accounting for ports operating in the Authenticator role. The accounting information sent by the switch to a RADIUS server includes the date and time when clients log on and log off, as well as the number of packets sent and received by a switch port during a client session. For background information on this feature, refer to Chapter 29, “802.1x Port-based Network Access Control” in the *AT-S63 Management Software Menus Interface User’s Guide*. This feature is disabled by default on the switch.

Configuring RADIUS Accounting

To configure RADIUS accounting, perform the following procedure:

- 1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

- 2. From the Configuration menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 137.

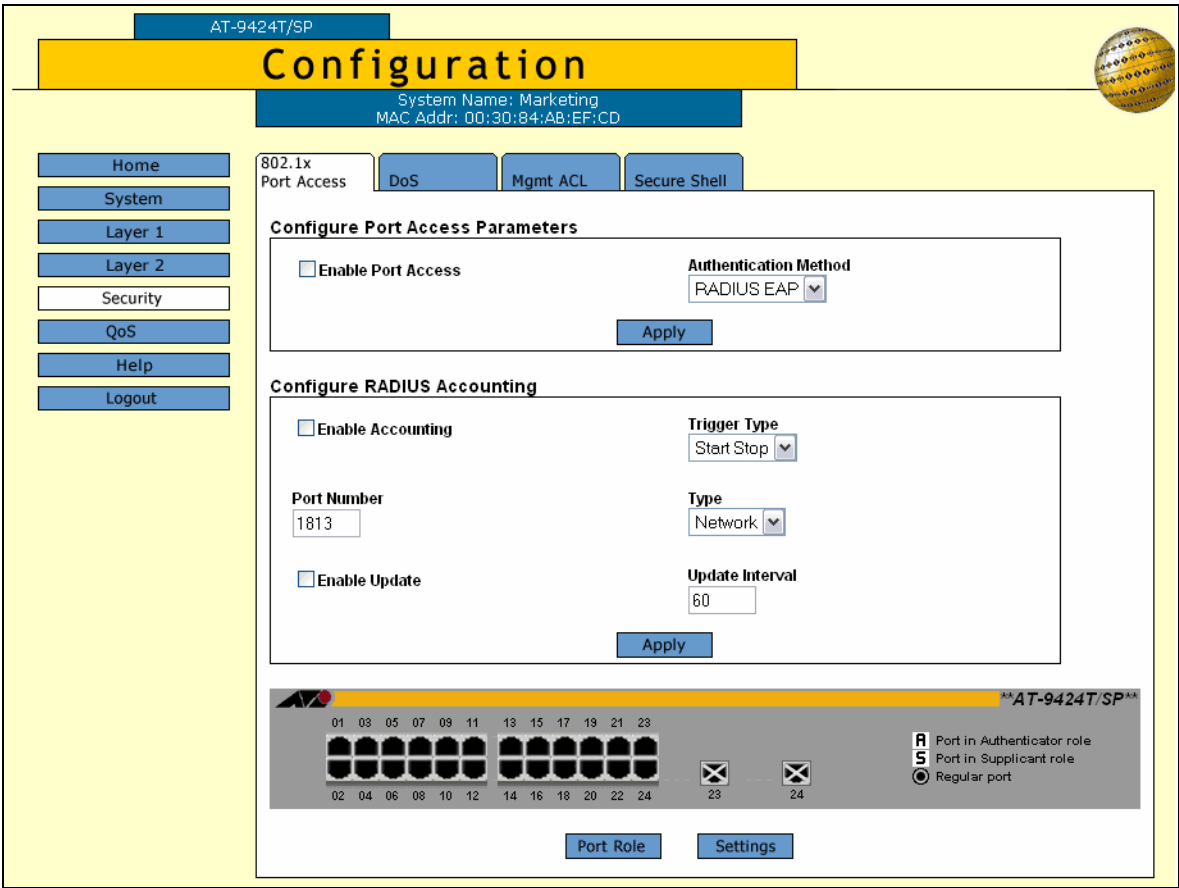


Figure 137. 802.1x Port Access Tab (Configuration)

3. In the Configure RADIUS Accounting section, adjust the following parameters as necessary.

Enable Accounting

This parameter activates or deactivates RADIUS accounting on the switch. Select Enabled to activate the feature or Disabled to deactivate it. The default is Disabled.

Trigger Type

This parameter specifies the action that causes the switch to send accounting information to the RADIUS server. The possible settings are:

Start_Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

Stop - The switch sends accounting information only when a client logs off.

Port Number

Specifies the UDP port for RADIUS accounting. The default is port 1813.

Type

This parameter specifies the type of RADIUS accounting. The default is Network. You cannot change this value.

Enable Update

This parameter controls whether the switch is to send interim accounting updates to the RADIUS server. A check in the box indicates that updating is enabled. No check in the box means that updating is disabled.

Update Interval

Specifies the intervals at which the switch sends interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

4. Click **Apply**.

Displaying the RADIUS Accounting Settings

To display the RADIUS accounting settings, perform the following procedure:

1. From the home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Monitoring menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 138.

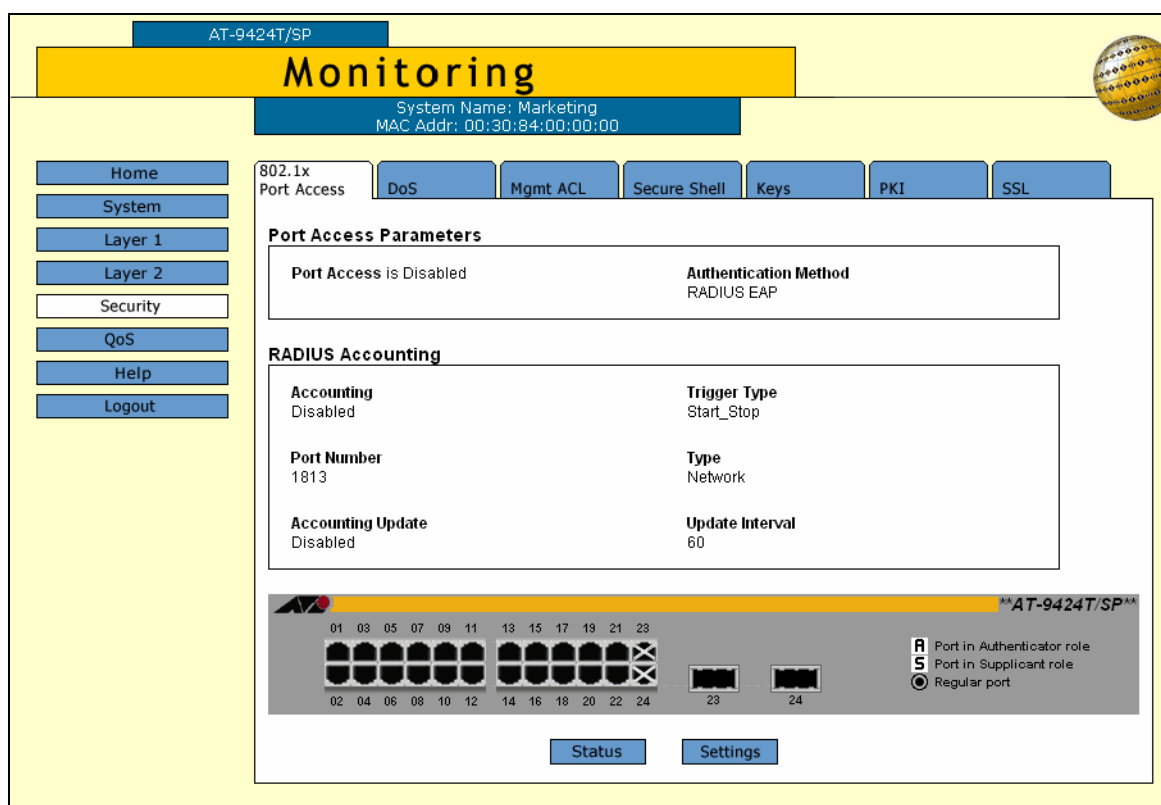


Figure 138. 802.1x Port Access Tab (Monitoring)

The RADIUS Accounting section provides the following information:

Accounting

The status of RADIUS accounting, either Enabled or Disabled.

Trigger Type

The action that causes the switch to send accounting information to the RADIUS server. The possible settings are:

Start_Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

Stop - The switch sends accounting information only when a client logs off.

Port Number

The UDP port for RADIUS accounting.

Type

The type of RADIUS accounting. The default is Network.

Accounting Update

Whether or not the switch sends interim accounting updates to the RADIUS server. The options are Enabled or Disabled.

Update Interval

The intervals, in seconds, at which the switch sends interim accounting updates to the RADIUS server.

The graphical image of the switch and the Status and Settings buttons refer to the 802.1x Port-based Network Access Control settings, described in "Displaying the Port-based Network Access Control Parameters" on page 342.

Chapter 24

Denial of Service Defense

This chapter contains instructions on how to configure the Denial of Service defense feature on the switch. The sections include:

- ❑ "Configuring Denial of Service Defense" on page 352
- ❑ "Displaying the DoS Settings" on page 355

Note

For background information on denial of service defense, refer to Chapter 31, "Denial of Service Defense," in the *AT-S63 Management Software Menus Interface User's Guide*.

Configuring Denial of Service Defense

To configure the ports on the switch for Denial of Service attack defense, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Security** option.

The Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 129 on page 334.

3. Select the **DoS** tab.

The DoS tab is shown in Figure 139.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:00:00:00

802.1x Port Access | **DoS** | Mgmt ACL | Secure Shell

DoS LAN Subnet IP: 0 . 0 . 0 . 0

DoS LAN Subnet Mask: 0 . 0 . 0 . 0

DoS Uplink Port: 24

Apply

AT-9424T/SP

01	03	05	07	09	11	13	15	17	19	21	23	02	04	06	08	10	12	14	16	18	20	22	24	23	24	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DoS Type: Syn Flood

Modify Modify All

Legend:
☒ Port is active
☐ Port is inactive
☒ Port is disabled
☐ Port is selected

Figure 139. DoS Tab (Configuration)

4. If you are implementing the SMURF or Land defense, you must provide an IP address and mask for your LAN. To do this, complete the following procedure: Otherwise, skip ahead to Step 5.
 - a. In the DoS LAN Subnet IP field, enter the IP address of one of the devices connected to the switch, preferably the lowest IP address.

- b. In the DoS Subnet Mask field, enter the LAN's mask. enter the mask. A binary "1" indicates the switch should filter on the corresponding bit of the IP address, while a "0" indicates that it should not. As an example, assume that the devices connected to a switch are using the IP address range 149.11.11.1 to 149.11.11.50. The mask would be 0.0.0.63.
 - c. If you are activating the Land defense, in the DoS Uplink Port field enter the number of the port connected to the device (e.g., DSL router) that leads outside your network. You can specify only one uplink port.
5. Click the ports in the switch image where you want to enable or disable a defense mechanism.
6. Using the DoS Type list, select the type of denial of service attack you want to either enable or disable on the ports. The possible selections are:
 - ☐ Syn Flood attack
 - ☐ Smurf attack
 - ☐ Land attack
 - ☐ Tear drop attack
 - ☐ Ping of death attack
 - ☐ IP Options
7. Click **Modify**. To configure all the ports, click **Modify All**.

The DoS Configuration for Ports page opens, as shown in Figure 140.

Figure 140. DoS Configuration for Ports Page

8. Adjust the settings as needed. The parameters are described below.

Status

Click Enable or Disable to enable or disable DoS on the selected ports.

Action

The action a port takes when an intruder packet is received. Although five possible selections are shown in the Action list box, they all do the same thing: block the packet, record the event, and drop the packet.

Mirror Port

This option applies to the Land, Tear Drop, Ping of Death, and IP Options. You can use this option to copy offending traffic to another port on the switch. You can specify only one mirror port. Specifying a mirror port is not required.

9. Click **Apply**.

The defense is immediately activated on the ports.

10. To permanently save the change, return to the General tab on the System page and click **Save Changes**.

For more information about what the Save Changes button does, refer to "Saving Your Parameter Changes" on page 36.

Displaying the DoS Settings

To display the DoS settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44

2. From the Monitoring menu, select the **Security** option.

The Security page opens with the 802.1x Port Access tab selected by default, as shown in Figure 133 on page 342.

3. Select the **DoS** tab.

The DoS tab is shown in Figure 141.

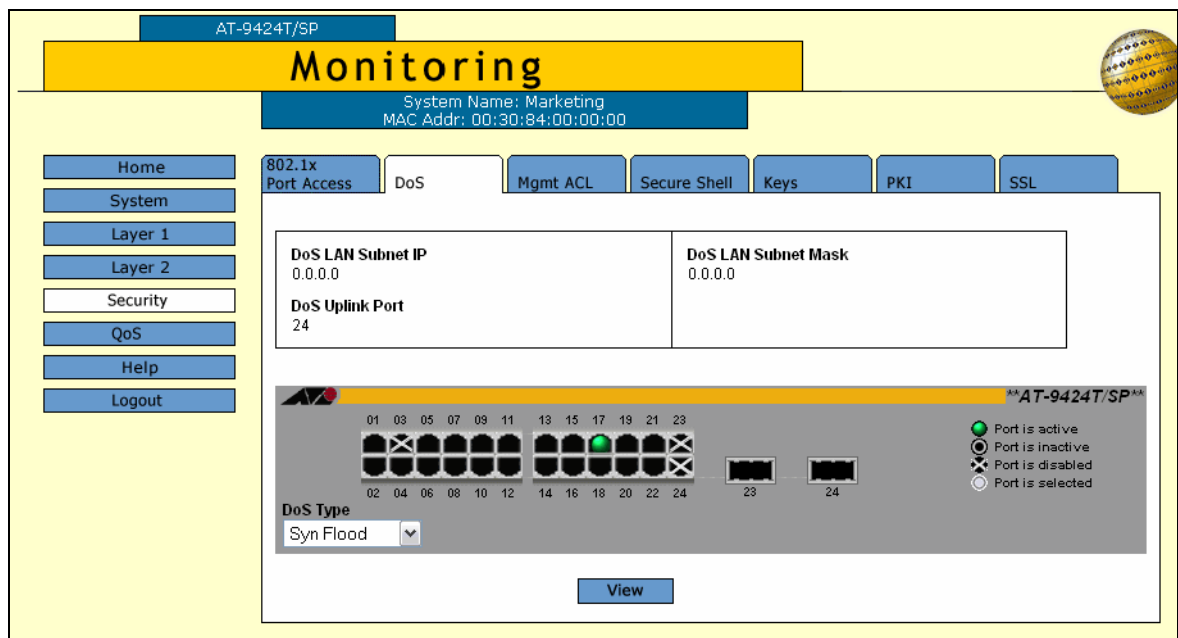
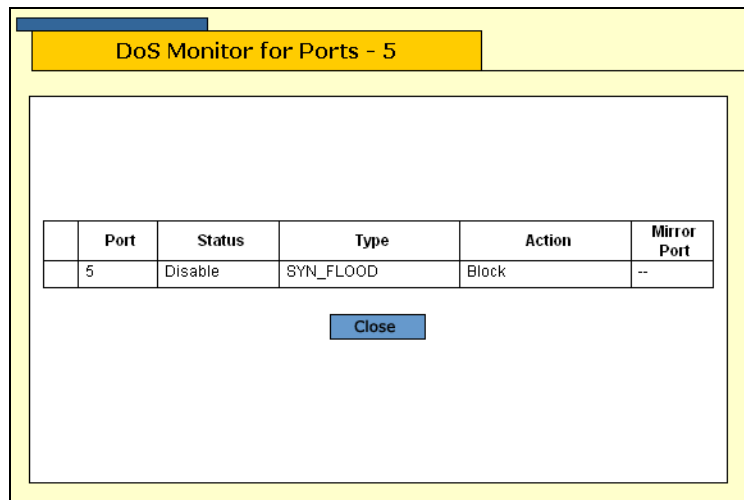


Figure 141. DoS Tab (Monitoring)

4. Click the port whose DoS settings you want to view. You can select more than one port at a time.
5. Using the DoS Type list, select the type of denial of service defense whose settings you want to view.
6. Click **View**.

The DoS Monitor for Port page opens, as shown in Figure 142.



Port	Status	Type	Action	Mirror Port
5	Disable	SYN_FLOOD	Block	--

Close

Figure 142. DoS Monitor for Ports Page

The page displays a table that contains the following columns of information:

Port

The port number.

Status

Whether DoS is enabled or disabled on the port.

Type

The type of DoS prevention.

Action

The action a port takes when an intruder packet is received. Although five possible actions may be shown, they all do the same thing: block the packet, record the event, and drop the packet.

Mirror Port

The port on the switch to which offending traffic is copied.

Appendix A

AT-S63 Default Settings

This appendix lists the AT-S63 factory default settings. It contains the following sections in alphabetical order:

- ☐ "Basic Switch Default Settings" on page 359
- ☐ "Enhanced Stacking Default Setting" on page 362
- ☐ "SNMP Default Settings" on page 363
- ☐ "Port Configuration Default Settings" on page 364
- ☐ "Event Log Default Settings" on page 365
- ☐ "Quality of Service" on page 366
- ☐ "IGMP Snooping Default Settings" on page 367
- ☐ "Denial of Service Prevention Default Settings" on page 368
- ☐ "STP, RSTP, and MSTP Default Settings" on page 369
- ☐ "VLAN Default Settings" on page 371
- ☐ "GVRP Default Settings" on page 372
- ☐ "Port Security Default Settings" on page 373
- ☐ "802.1x Port-Based Network Access Control Default Settings" on page 374
- ☐ "Web Server Default Settings" on page 375
- ☐ "SSL Default Settings" on page 376
- ☐ "PKI Default Settings" on page 377
- ☐ "SSH Default Settings" on page 378
- ☐ "Server-Based Authentication Default Settings" on page 379

- ❑ "Management Access Control List Default Setting" on page 380

Basic Switch Default Settings

This section lists the default settings for basic switch parameters. The following topics are covered:

- ☐ "Boot Configuration File Default Setting" on page 359
- ☐ "Management Access Default Settings" on page 359
- ☐ "Management Interface Default Settings" on page 359
- ☐ "RJ-45 Serial Terminal Port Default Settings" on page 360
- ☐ "SNTP Default Settings" on page 360
- ☐ "Switch Administration Default Settings" on page 361
- ☐ "System Software Default Settings" on page 361

Boot Configuration File Default Setting

The following table lists the File menu default setting.

File Menu Setting	Default
Default Configuration File	boot.cfg

Management Access Default Settings

The following table lists the management access default settings.

Remote Management Access Setting	Default
Telnet	Enabled
SNMP	Disabled
TFTP	Enabled
Web Server	Enabled

Management Interface Default Settings

The following table lists the management interface default settings.

Management Interface Setting	Default
Manager Login Name	manager
Manager Password	friend
Operator Login Name	operator
Operator Password	operator

Management Interface Setting	Default
Console Disconnect Timer Interval	10 minutes

Note

Login names and passwords are case sensitive.

RJ-45 Serial Terminal Port Default Settings

The following table lists the RJ-45 serial terminal port default settings.

RJ-45 Port Setting	Default
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Baud Rate	9600 bps

SNTP Default Settings

The following table lists the SNTP default settings.

SNTP Setting	Default
System Time	00:00:00 on January 1, 1970
SNTP Status	Disabled
SNTP Server	0.0.0.0
UTC Offset	+0
Daylight Savings Time (DST)	Enabled
Poll Interval	600 seconds

Switch Administration Default Settings

The following table describes the switch administration default settings.

Administration Setting	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
System Name	None
Administrator	None
Comments	None
BOOTP/DHCP	Disabled
MAC Address Aging Time	300 seconds

System Software Default Settings

The following table lists the system software default settings.

System Software Setting	Default
Console Startup Mode	CLI

Enhanced Stacking Default Setting

The following table lists the enhanced stacking default setting.

Enhanced Stacking Setting	Default
Switch State	Slave

SNMP Default Settings

The following table describes the SNMP default settings.

SNMP Communities Setting	Default
SNMP Status	Disabled
Authentication Failure Trap Status	Disabled
Community Name	public (Read only)
Community Name	private (Read Write)
Status (public)	Enabled
Status (private)	Enabled
Open Status (public)	Yes
Open Status (private)	Yes

Port Configuration Default Settings

The following table lists the port configuration default settings.

Port Configuration Setting	Default
Status	Enabled
Broadcast Filter	Disabled
Override Priority	No override
HOL Blocking	Disabled
Back Pressure	Disabled
Flow Control	Auto
Speed	Auto-Negotiation
Duplex Mode	Auto-Negotiation
MDI/MDI-X	Auto-MDI/MDIX

Event Log Default Settings

The following table lists the event log default settings.

Event Log Setting	Default
Status	Enabled
Full Log Action	Wrap

Quality of Service

The following table lists the default mappings of IEEE 802.1p priority levels to egress port priority queues

IEEE 802.1p Priority Level	Port Priority Queue
0 or 1	Q0 (lowest)
2 or 3	Q1
4 or 5	Q2
6 or 7	Q3 (highest)

IGMP Snooping Default Settings

The following table lists the IGMP Snooping default settings.

IGMP Snooping Setting	Default
IGMP Snooping Status	Disabled
Multicast Host Topology	Single Host/ Port (Edge)
Host/Router Timeout Interval	260 seconds
Maximum Multicast Groups	64
Multicast Router Ports Mode	Auto Detect

Denial of Service Prevention Default Settings

The following table lists the default settings for the Denial of Service prevention feature.

Denial of Service Prevention Setting	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Uplink Port	26
SYN Flood Defense	Disabled
Smurf Defense	Disabled
Land Defense	Disabled
Teardrop Defense	Disabled
Ping of Death Defense	Disabled
IP Options Defense	Disabled

STP, RSTP, and MSTP Default Settings

This section provides the spanning tree, STP RSTP, and MSTP, default settings.

Spanning Tree Switch Settings

The following table describes the Spanning Tree Protocol default settings for the switch.

STP Switch Setting	Default
Spanning Tree Status	Disabled
Active Protocol Version	RSTP

STP Default Settings

The following table describes the STP default settings.

STP Setting	Default
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Port Cost	Automatic -Update
Port Priority	128

RSTP Default Settings

The following table describes the RSTP default settings.

RSTP Setting	Default
Force Version	RSTP
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Edge Port	Yes
Point-to-Point	Auto Detect
Port Cost	Automatic Update

RSTP Setting	Default
Port Priority	128

MSTP Default Settings

The following table lists the MSTP default settings.

MSTP Setting	Default
Status	Disabled
Force Version	MSTP
Bridge Hello Time	2
Bridge Forwarding Delay	15
Bridge Max Age	20
Maximum Hops	20
Configuration Name	null
Revision Level	0
CIST Priority	Increment 8 (32768)
Port Priority	Increment 8 (128)
Port Internal Path Cost	Auto Update
Port External Path Cost	200,000
Point-to-Point	Auto Detect
Edge Port	Yes

VLAN Default Settings

This section provides VLAN default settings.

VLAN Setting	Default
Default VLAN Name	Default_VLAN (all ports)
Management VLAN ID	1 (Default_VLAN)
VLAN Mode	User Configured
Uplink Port	None

GVRP Default Settings

This section provides the default settings for GVRP.

GVRP Setting	Default
Status	Disabled
GIP Status	Enabled
Join Timer	20 centiseconds
Leave Timer	60 centiseconds
Leave All Timer	1000 centiseconds
Port Mode	Normal

Port Security Default Settings

The following table lists the port security default settings.

Port Security Setting	Default
Security Mode	Automatic (no security)
Intrusion Action	Discard
Participating	No
MAC Limit	No Limit

802.1x Port-Based Network Access Control Default Settings

The following table describes the 802.1x Port-based Network Access Control default settings.

802.1x Port-based Network Access Control Settings	Default
Port Access Control	Disabled
Authentication Method	RADIUS EAP
Port Role	None

The following table lists the default settings for RADIUS accounting.

RADIUS Accounting Settings	Default
Status	Disabled
Port	1813
Type	Network
Trigger Type	Start_Stop
Update Status	Disabled
Update Interval	60

Web Server Default Settings

The following table lists the web server default settings.

Web Server Configuration Setting	Default
Status	Enabled
Mode	HTTP
Port Number	80
SSL Key ID	None

SSL Default Settings

The following table lists the SSL default settings.

SSL Setting	Default
Maximum Number of Sessions	50
Session Cache Timeout	300 seconds

PKI Default Settings

The following table lists the PKI default settings, including the generate enrollment request settings.

PKI Setting	Default
Switch Distinguished Name	None
Maximum Number of Certificates	256
Request Name	None
Key Pair ID	0
Format	PEM
Type	PKCS10

SSH Default Settings

The following table lists the SSH default settings.

SSH Setting	Default
Status	Disabled
Host Key ID	Not Defined
Server Key ID	Not Defined
Server Key Expiry Time	0 hours
Login Timeout	180 seconds

Server-Based Authentication Default Settings

This section describes the server-based authentication, RADIUS, and TACACS+ client default settings.

Server-Based Authentication Default Settings

The following table describes the server-based authentication default settings.

Server-based Authentication Setting	Default
Server-based Authentication	Disabled
Active Authentication Method	TACACS+

RADIUS Default Settings

The following table lists the RADIUS configuration default settings.

RADIUS Configuration Setting	Default
Global Encryption Key	ATI
Global Server Timeout Period	30 seconds
RADIUS Server 1 Configuration	0.0.0.0
RADIUS Server 2 Configuration	0.0.0.0
RADIUS Server 3 Configuration	0.0.0.0
Auth Port	1812
Encryption Key	Not Defined

TACACS+ Client Default Settings

The following table lists the TACACS+ client configuration default settings.

TACACS+ Client Configuration Setting	Default
TAC Server 1	0.0.0.0
TAC Server 2	0.0.0.0
TAC Server 3	0.0.0.0
TAC Server Order	1 2 3
TAC Global Secret	None
TAC Timeout	30 seconds

Management Access Control List Default Setting

The following table lists the default setting for the Management Access Control List.

Management ACL Setting	Default
Status	Disabled

Index

Numerics

- 802.1x Port-based Network Access Control
 - access role, configuring 334
 - authenticator port, configuring 337
 - configuring 334
 - default settings 374
 - disabling 336
 - enabling 336
 - port parameters, displaying 343
 - port role, configuring 334
 - port status, displaying 342
 - supplicant port, configuring 340

A

- administrator name
 - configuring 41
 - default setting 361
- aging time
 - changing 97
 - default setting 361
- app (applicant state machine) 294
- associations, VLANs to MSTI IDs 192
- AT-S63 software
 - default settings 357
 - resetting to factory defaults 50
- AT-S63 software updates
 - downloading 20
 - obtaining 20
- auth period 341
- authentication failure trap, default setting 363
- authentication protocols, enabling or disabling 324
- autonegotiation, configuring 76

B

- back pressure
 - configuring 78
 - default setting 364
- Boot Protocol (BootP)
 - activating 43
 - default setting 361
- bridge forwarding delay
 - default setting 369
 - Multiple Spanning Tree Protocol (MSTP) 186
 - Rapid Spanning Tree Protocol (RSTP) 176
 - Spanning Tree Protocol (STP) 168
- bridge hello time
 - default setting 369
 - Multiple Spanning Tree Protocol (MSTP) 186
 - Rapid Spanning Tree Protocol (RSTP) 176
 - Spanning Tree Protocol (STP) 168
- bridge identifier
 - Rapid Spanning Tree Protocol (RSTP) 176
 - Spanning Tree Protocol (STP) 169
- bridge max age
 - default setting 369
 - Multiple Spanning Tree Protocol (MSTP) 186
 - Rapid Spanning Tree Protocol (RSTP) 176
 - Spanning Tree Protocol (STP) 168
- bridge priority
 - default setting 369
 - Rapid Spanning Tree Protocol (RSTP) 175
 - Spanning Tree Protocol (STP) 167
- bridge protocol data unit (BPDU) 176
- broadcast filter, default setting 364
- browser tools 35

C

- ciphers available parameter 321
- CIST priority parameter 187
- Class of Service (CoS)
 - configuring 142
 - mapping to egress queues 145
 - schedule, displaying 152
 - scheduling, configuring 148
 - settings, displaying 150
- Common and Internal Spanning Tree (CIST), configuring 187
- community name
 - SNMPv1 and SNMPv2c 57
 - SNMPv3 protocol 253, 256
- configuration file, default name 359
- console disconnect interval, default setting 360
- console startup mode, default setting 361

D

- data compression parameter 321
- daylight savings time (DST), default setting 360
- default values, AT-S63 software 357
- Denial of Service (DoS) defense
 - configuring 352
 - default settings 368
 - enabling or disabling 354
 - mirror port 354
 - settings, displaying 355
- distinguished name, default setting 377
- document conventions 17
- documentation 18
- duplex mode
 - configuring 76
 - default setting 364
- Dynamic Host Control Protocol (DHCP)
 - activating 43
 - default setting 361

E

- edge port
 - default setting 369
 - Multiple Spanning Tree Protocol (MSTP) 196
- encryption keys, displaying 310
- enhanced stacking
 - changing switches 68
 - configuring 66
 - default switch setting 362
 - setting switch status 66
- event log
 - clearing 138
 - default settings 365

- disabling 128, 137
- displaying 130
- enabling 128
- saving to a file 139
- severity codes 134
- software module list 132

F

- factory defaults
 - list 357
 - resetting switch 50
- flow control
 - configuring 77
 - default setting 364
- force version
 - default setting 369
 - Multiple Spanning Tree Protocol (MSTP) 186
 - Rapid Spanning Tree Protocol (RSTP) 175

G

- GARP VLAN Registration Protocol (GVRP)
 - configuration, displaying 289
 - configuring 286
 - counters, displaying 296
 - database, displaying 292
 - default settings 372
 - disabling 288
 - enabling 288
 - GIP connected ports ring, displaying 300
 - GVRP state machine, displaying 293
 - port configuration, displaying 291
- gateway address
 - configuring 42
 - default setting 361
 - displaying 45
- global encryption key
 - configuring 329, 331
 - default setting 379
- global secret
 - configuring 325, 328
 - default setting 379
- global server timeout
 - configuring 325, 328
 - default setting 379
- GVRP. *See* GARP VLAN Registration Protocol (GVRP)

H

- hardware information 44
- held period 341
- hello time
 - default setting 369

- Rapid Spanning Tree Protocol (RSTP) 176
- Spanning Tree Protocol (STP) 168
- HOL blocking, default setting 364
- host key ID parameter 318
- host nodes, displaying 157
- host/router timeout interval
 - configuring 155, 158
 - default setting 367

I

- ingress packet threshold 78
- Internet Group Management Protocol (IGMP)
 - snooping
 - configuring 154
 - default settings 367
 - disabling 154, 157
 - displaying 157
 - enabling 154, 157
- Internet Protocol (IP) address
 - configuring 42
 - default 361
- intrusion action (port)
 - configuring 307
 - default setting 373

L

- local management session, definition 24
- login timeout parameter 319

M

- MAC address aging time
 - changing 97
 - default setting 361
- MAC address table, displaying 94
- MAC addresses
 - adding 90
 - deleting dynamic 93
 - deleting multicast 92
 - displaying 94
- MAC limit, default setting 373
- MACs available parameter 321
- Management Access Control List, default setting 380
- management access defaults 359
- management access levels 28, 46
- Management Information Base. *See* MIBs
- management interface defaults 359
- management VLAN ID
 - configuring 283
 - default setting 371
- management VLAN, specifying 283

- manager access 28, 46
- manager password
 - configuring 46
 - default setting 359
- master switch
 - assigning 66
 - defined 66
 - returning to 71
- max age
 - default setting 369
 - Rapid Spanning Tree Protocol (RSTP) 176
 - Spanning Tree Protocol (STP) 168
- max hops, Multiple Spanning Tree Protocol (MSTP) 187
- max requests 339
- max start 341
- maximum multicast groups
 - configuring 155
 - default setting 367
 - displaying 158
- maximum number of sessions, default setting 376
- MDI/MDIX mode 79
- MIBs, supported 27
- MSTI ID
 - creating 189
 - deleting 190
 - modifying 190
- MSTI ID association to a VLAN
 - adding 192
 - modifying 193
- MSTI. <italic>See Multiple Spanning Tree Instance (MSTI)</italic>
- multicast groups, maximum
 - configuring 155
 - displaying 158
- multicast host topology
 - configuring 154
 - default setting 367
 - displaying 157
- multicast MAC address
 - adding 90
 - deleting 92
 - displaying 94
- multicast router ports
 - configuring 155, 158
 - default setting 367
- multicast routers, displaying 160
- Multiple Spanning Tree Instance (MSTI)
 - associating to VLANs 192
 - disassociating from VLANs 192
 - modifying association to VLANs 193

- MSTI ID
 - creating 189
 - deleting 190
 - modifying 190
 - removing a VLAN association 192
- Multiple Spanning Tree Protocol (MSTP)
 - associating VLANs to MSTI IDs 192
 - bridge forwarding delay 186
 - bridge hello time 186
 - bridge max age 186
 - bridge settings, configuring 184
 - configuration name 186
 - configuring 184
 - connecting to VLANs 192
 - default settings 370
 - disabling 182
 - edge port 196
 - enabling 182
 - force version 186
 - max hops 187
 - MSTI ID
 - creating 189
 - deleting 190
 - modifying 190
 - parameters
 - configuring 184
 - parameters, displaying 197
 - point-to-point port 196
 - port external path cost 196
 - port internal path cost 196
 - port parameters
 - configuring 195
 - displaying 197
 - port priority 195
 - port settings, displaying 200
 - port status, displaying 200
 - resetting to defaults 202
- O**
 - operator access 28, 46
 - operator password
 - configuring 46
 - default setting 359
 - override priority, default setting 364
- P**
 - password
 - changing 46
 - default 33
 - pinging 49
 - PKI certificates, maximum number, default setting 377
 - point-to-point port
 - default setting 369
 - Multiple Spanning Tree Protocol (MSTP) 196
 - Rapid Spanning Tree Protocol (RSTP) 177
 - poll interval, default setting 360
 - port
 - configuring parameters, basic 74
 - disabling 75
 - enabling 75
 - link status 82
 - resetting to defaults 88
 - statistics, displaying 85
 - status
 - default setting 364
 - displaying 81
 - port control
 - 802.1x port-based access control 338
 - force-authorized 338
 - force-unauthorized 338
 - port cost
 - default setting 369
 - Multiple Spanning Tree Protocol (MSTP) 196
 - Rapid Spanning Tree Protocol (RSTP) 177
 - Spanning Tree Protocol (STP) 170
 - port mirror
 - creating 110
 - deleting 115
 - disabling 114
 - displaying 116
 - modifying 113
 - port parameters, configuring
 - basic 74
 - Multiple Spanning Tree Protocol (MSTP) 184
 - Rapid Spanning Tree Protocol (RSTP) 174
 - Spanning Tree Protocol (STP) 166
 - port priority
 - default setting 369
 - Multiple Spanning Tree Protocol (MSTP) 195
 - Rapid Spanning Tree Protocol (RSTP) 177
 - Spanning Tree Protocol (STP) 169
 - port role, default setting 374
 - port security
 - default settings 373
 - displaying 306
 - intrusion action 307
 - port speed
 - configuring 76
 - default setting 364
 - port trunk
 - creating 100

- deleting 105
- displaying 106
- modifying 103
- port-based VLAN
 - creating 272
 - deleting 278
 - displaying 281
 - modifying 276
- Public Key Infrastructure (PKI)
 - default settings 377
 - settings, displaying 312

Q

Quality of Service (QoS), default settings 366

quiet period, configuring 338

R**RADIUS**

- configuring 329
- default settings 379
- disabling 324
- displaying settings 331
- enabling 324
- server timeout 332

RADIUS accounting

- configuring 346
- settings, displaying 347

RADIUS server

- encryption secret 330
- encryption secret, configuring 326
- IP address, configuring 330

Rapid Spanning Tree Protocol (RSTP)

- bridge forwarding delay 176
- bridge hello time 176
- bridge identifier 176
- bridge max age 176
- bridge priority 175
- bridge settings, configuring 174
- default settings 369
- disabling 164, 182
- edge port, configuring 177
- enabling 164, 182
- force version 175
- parameters, displaying 170, 197
- point-to-point port, configuring 177
- port cost 177
- port priority 177
- port settings, displaying 178, 200
- resetting to defaults 178

rate limit, setting 78

reauth period, configuring 338

reg (registrar state machine) parameter 295

remote management access defaults 359

RJ-45 serial terminal port, default settings 360

S**Secure Shell (SSH) protocol**

- configuring 318
- default settings 378
- displaying settings 320

Secure Sockets Layer (SSL)

- default settings 376
- displaying settings 315

server authentication UDP port

- configuring 330
- default setting 379

server key ID parameter 318**server timeout, configuring 338****server-based authentication method, default setting 379****session cache timeout**

- configuring 315
- default setting 376

Simple Network Time Protocol (SNTP), default setting 360**slave switch**

- assigning 66
- defined 66

SNMP

- default setting for remote management 359
- default settings 363

SNMP community string, default name 363**SNMP management**

- disabling 54, 205
- enabling 54, 205

SNMP management session 27**SNMP management, default setting 363****SNMPv1 and SNMPv2c community**

- creating 56
- deleting 61
- displaying 62
- modifying 59

SNMPv3 Access Table entry

- creating 220
- deleting 224
- displaying 262
- modifying 224

SNMPv3 community name, modifying 256**SNMPv3 Community Table entry**

- creating 252
- deleting 255
- displaying 267

- modifying 255
- SNMPv3 Notify Table entry
 - creating 233
 - deleting 235
 - displaying 264
 - modifying 236
- SNMPv3 SecurityToGroup Table entry
 - creating 227
 - deleting 230
 - displaying 263
 - modifying 230
- SNMPv3 Target Address Table entry
 - creating 238
 - deleting 241
 - displaying 265
 - modifying 242
- SNMPv3 Target Parameters Table entry
 - creating 245
 - deleting 248
 - displaying 266
 - modifying 249
- SNMPv3 User Table entry
 - creating 207
 - deleting 210
 - displaying 259
 - modifying 211
- SNMPv3 View Table entry
 - creating 214
 - deleting 217
 - displaying 261
 - modifying 218
- SNTP server, default setting 360
- SNTP. *See* Simple Network Time Protocol (SNTP)
- software information 44
- Spanning Tree Protocol (STP)
 - bridge forwarding delay 168
 - bridge hello time 168
 - bridge identifier 169
 - bridge max age 168
 - bridge parameters, configuring 166
 - bridge priority 167
 - default settings 369
 - disabling 164, 182
 - enabling 164, 182
 - parameters
 - displaying 197
 - parameters, displaying 170
 - port cost 170
 - port priority 169
 - port settings, displaying 200
 - resetting to defaults 172

- spanning tree, default setting 369
- static MAC address
 - adding 90
 - deleting 92
- static unicast MAC address, displaying 94
- STP ID 300
- subnet mask
 - configuring 42
 - default setting 361
- supplicant port, start period 341
- supplicant timeout 338
- switch
 - hardware information 44
 - software information 44
- switch name, configuring 40
- switch state, default setting 362
- switch, rebooting 48
- system date, default setting 360
- system file
 - downloading 122
 - uploading 125
- system name
 - configuring 41
 - default setting 361
- system software default settings 361
- system time, default setting 360

T

- TACACS+
 - configuring 325
 - default settings 379
 - disabling 324
 - displaying settings 327
 - enabling 324
 - server timeout 329, 379
- tagged VLAN
 - creating 272
 - deleting 278
 - displaying 281
 - modifying 276
- Telnet management session, defined 25
- Telnet, default setting for remote management 359
- TFTP, default setting for remote management 359
- tx period, configuring 338

U

- unavailable status, defined 66
- uplink port
 - configuring 280
 - default setting 371
- user name

- configuring 341
- default 33
- user password, configuring 341
- UTC offset, default setting 360

V

- versions supported (SSH) parameter 320
- virtual LAN (VLAN)
 - associating to MSTI IDs 192
 - creating 272
 - default settings 371
 - deleting 278
 - displaying 281
 - mode, selecting 279
 - modifying 276
- VLAN name, default setting 371

W

- web browser management session
 - defined 26
 - limitations 26
 - quitting 37
 - starting 32
- web server, default settings 375

